[RENESAS SECURITY PROCESS INTRODUCTION TRAINING]

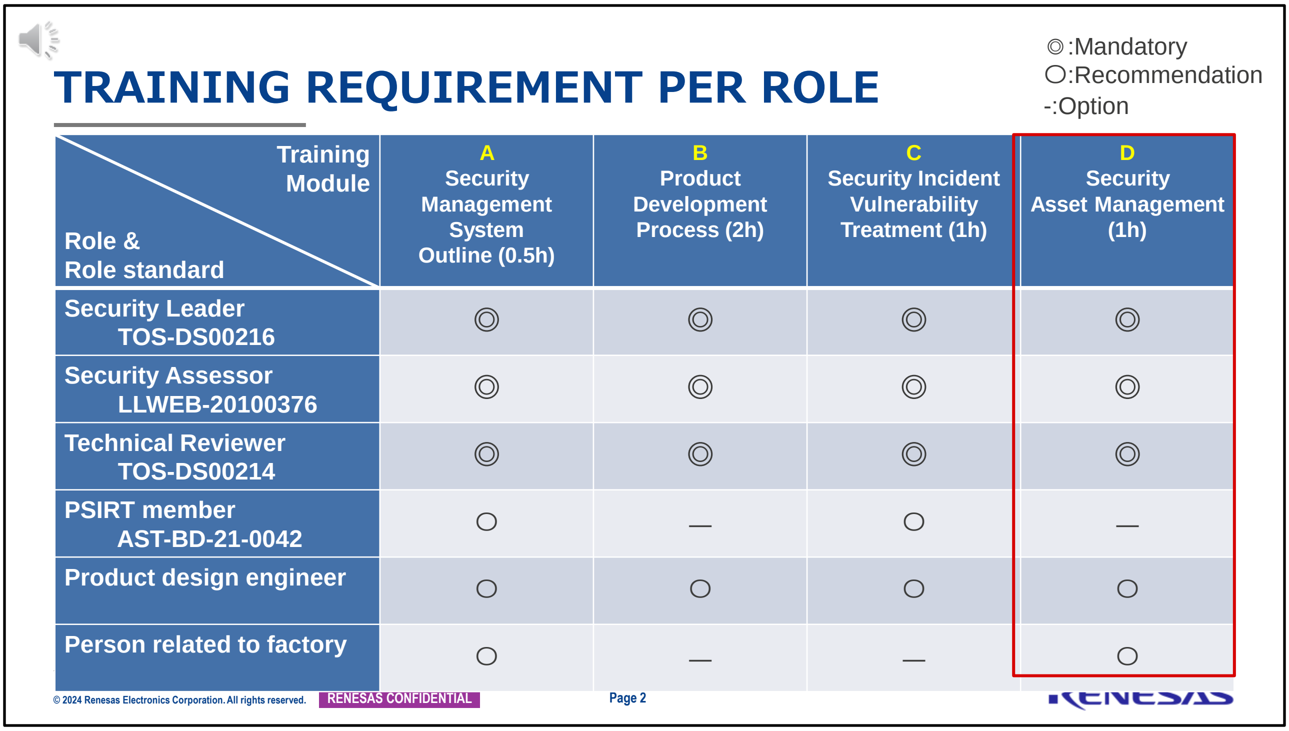
SECURITY ASSET MANAGEMENT

(RCT-JB0026, RCT-JB0027)

REV.3.0 3RD JUN. 2024 REL/QA/QAD/QSP/QDSC S. NAGATA, K. AMIMOTO

RENESAS CONFIDENTIAL

I will explain Renesas security asset management.



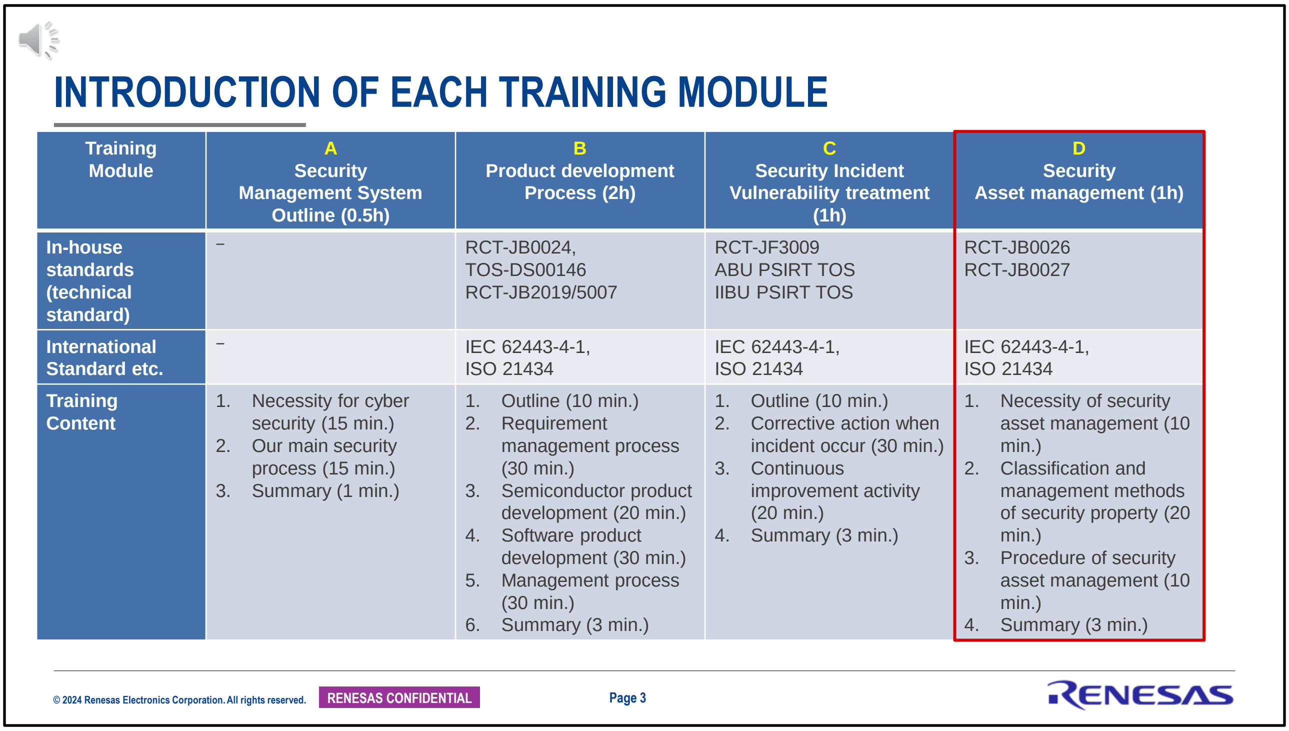
◎:Mandatory
○:Recommendation
-:Option

TRAINING REQUIREMENT PER ROLE

Training Module Role & Role standard	A Security Management System Outline (0.5h)	B Product Development Process (2h)	C Security Incident Vulnerability Treatment (1h)	D Security Asset Management (1h)
Security Leader TOS-DS00216	◎	◎	◎	◎
Security Assessor LLWEB-20100376	◎	◎	◎	◎
Technical Reviewer TOS-DS00214	◎	◎	◎	◎
PSIRT member AST-BD-21-0042	○	—	○	—
Product design engineer	○	○	○	○
Person related to factory	○	—	—	○

RENESAS CONFIDENTIAL Page 2

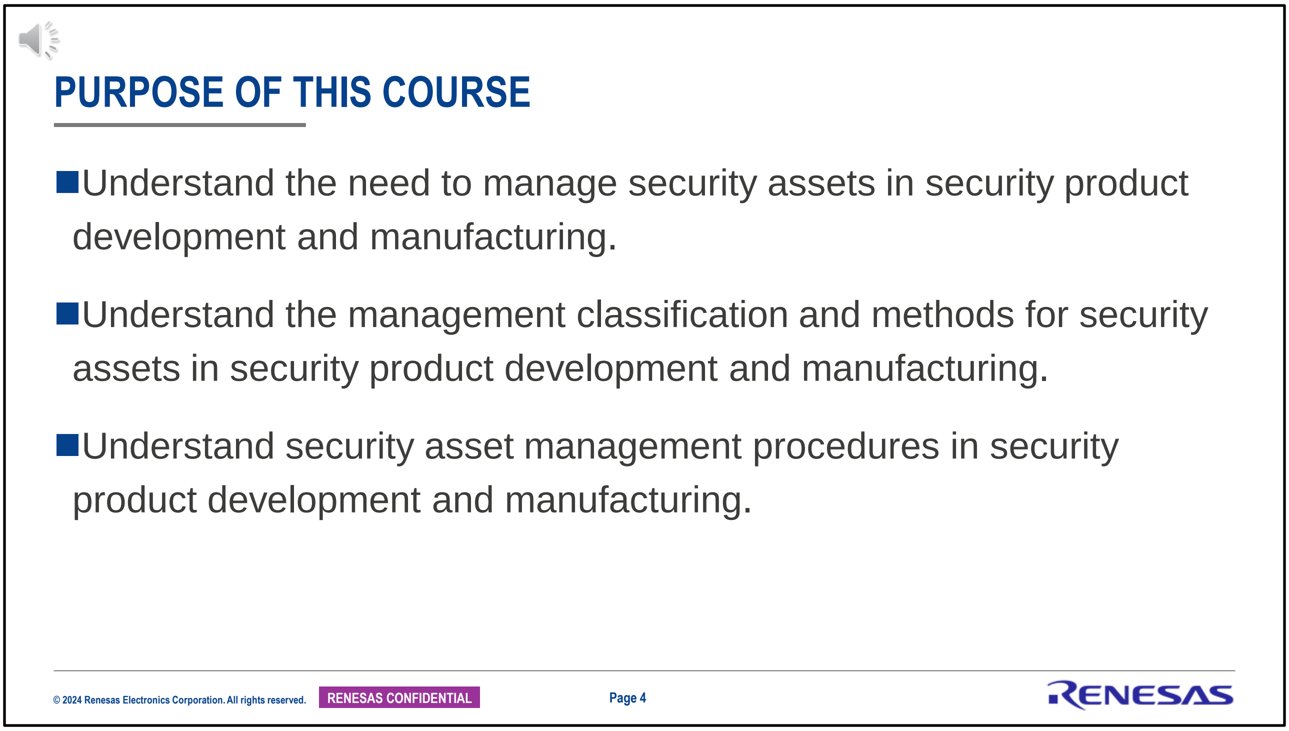
This table shows the relationship between the four security process basic course modules, including module D of this course, and whether or not those in each role need to take the course. I will omit the explanation because it has been already explained in the module course of C from A.



INTRODUCTION OF EACH TRAINING MODULE

Training Module	A Security Management System Outline (0.5h)	B Product development Process (2h)	C Security Incident Vulnerability treatment (1h)	D Security Asset management (1h)
In-house standards (technical standard)	–	RCT-JB0024, TOS-DS00146 RCT-JB2019/5007	RCT-JF3009 ABU PSIRT TOS IIBU PSIRT TOS	RCT-JB0026 RCT-JB0027
International Standard etc.	–	IEC 62443-4-1, ISO 21434	IEC 62443-4-1, ISO 21434	IEC 62443-4-1, ISO 21434
Training Content	1. Necessity for cyber security (15 min.) 2. Our main security process (15 min.) 3. Summary (1 min.)	1. Outline (10 min.) 2. Requirement management process (30 min.) 3. Semiconductor product development (20 min.) 4. Software product development (30 min.) 5. Management process (30 min.) 6. Summary (3 min.)	1. Outline (10 min.) 2. Corrective action when incident occur (30 min.) 3. Continuous improvement activity (20 min.) 4. Summary (3 min.)	1. Necessity of security asset management (10 min.) 2. Classification and management methods of security property (20 min.) 3. Procedure of security asset management (10 min.) 4. Summary (3 min.)

This is the time required for each module. I will omit the explanation.

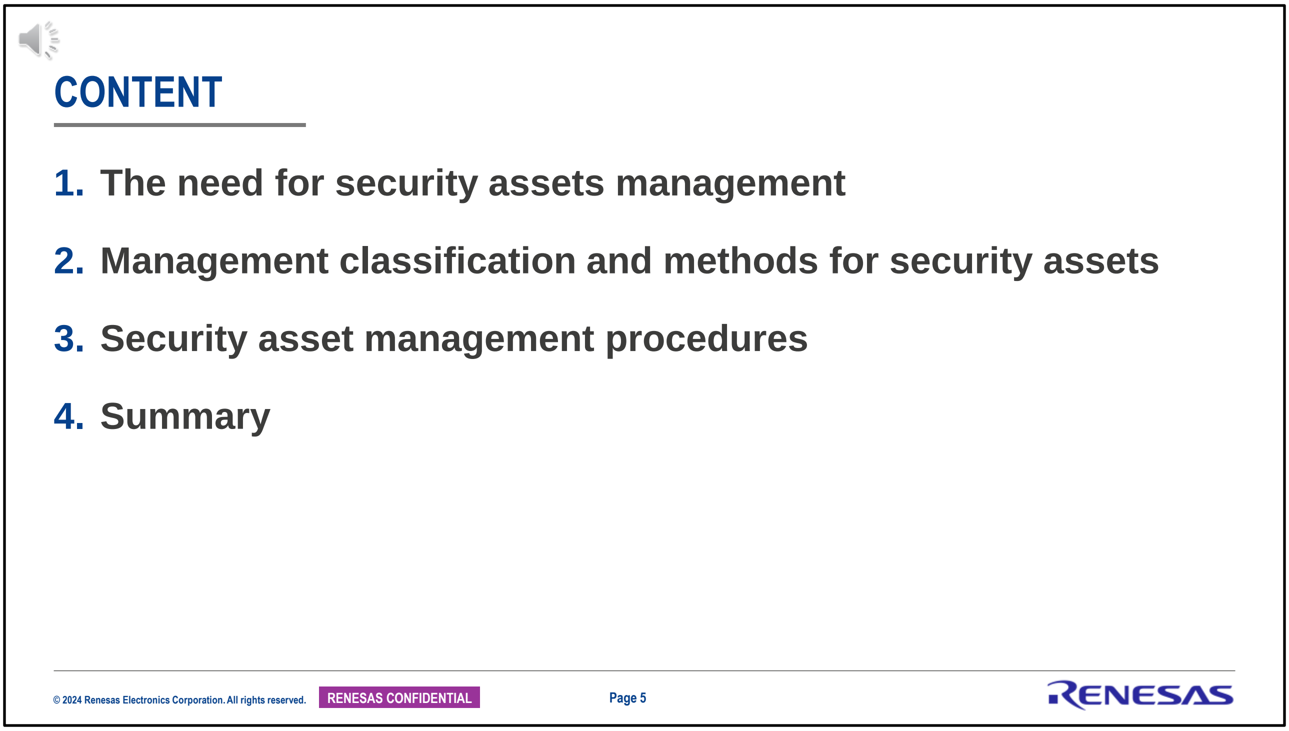


PURPOSE OF THIS COURSE

- Understand the need to manage security assets in security product development and manufacturing.
- Understand the management classification and methods for security assets in security product development and manufacturing.
- Understand security asset management procedures in security product development and manufacturing.

RENESAS CONFIDENTIAL

This is the purpose of this course. We will explain the necessity and specific procedures for security asset management, but the content will be a summary of RCT-JB0026 and 0027, which stipulate the rules for security asset management.



CONTENT

1. The need for security assets management
2. Management classification and methods for security assets
3. Security asset management procedures
4. Summary

RENESAS CONFIDENTIAL

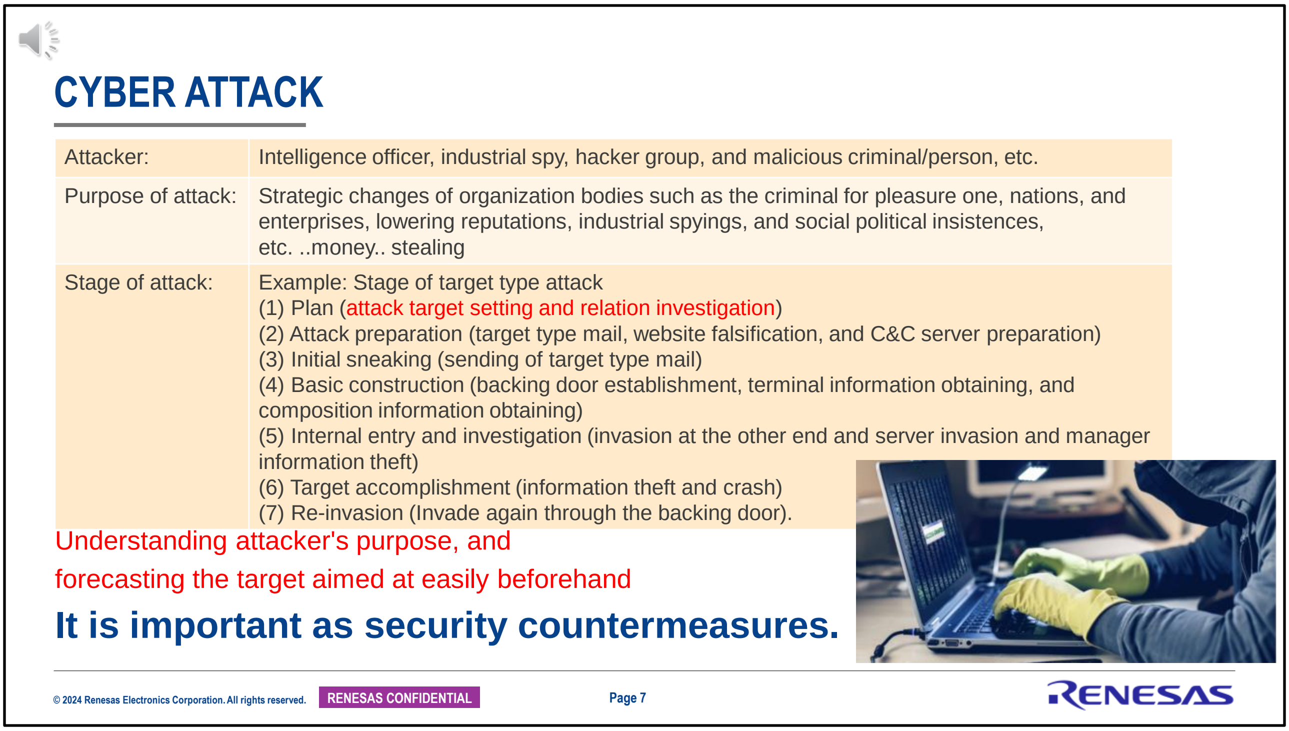
RENESAS

This is the chapters structure of this course. We will explain in order why security asset management is necessary, how it is performed, and where it is performed during each product development process.

1. THE NEED FOR SECURITY ASSETS MANAGEMENT

RENESAS CONFIDENTIAL

Chapter 1 is the necessity of security asset management.



CYBER ATTACK

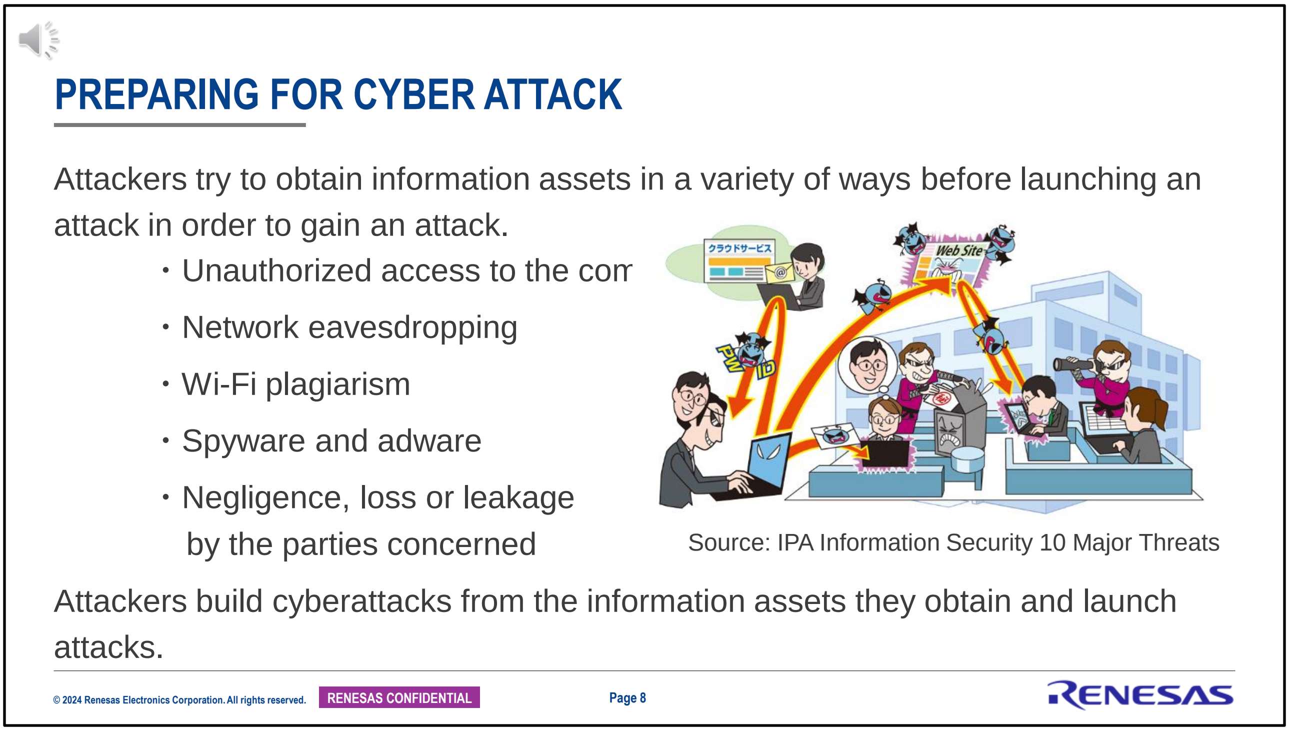
Attacker:	Intelligence officer, industrial spy, hacker group, and malicious criminal/person, etc.
Purpose of attack:	Strategic changes of organization bodies such as the criminal for pleasure one, nations, and enterprises, lowering reputations, industrial spyings, and social political insistences, etc. ..money.. stealing
Stage of attack:	Example: Stage of target type attack (1) Plan (attack target setting and relation investigation) (2) Attack preparation (target type mail, website falsification, and C&C server preparation) (3) Initial sneaking (sending of target type mail) (4) Basic construction (backing door establishment, terminal information obtaining, and composition information obtaining) (5) Internal entry and investigation (invasion at the other end and server invasion and manager information theft) (6) Target accomplishment (information theft and crash) (7) Re-invasion (Invade again through the backing door).

Understanding attacker's purpose, and forecasting the target aimed at easily beforehand

It is important as security countermeasures.

RENESAS CONFIDENTIAL Page 7 RENESAS

First, to understand why security asset management is necessary, we will start with an overview of cyber attacks. As shown in this table, an attacker first makes an attack plan, then prepares, executes, and withdraws according to that plan. To prevent this attack, it is necessary to predict the attacker's intentions and techniques in advance.


クラウドサービス
Web Site
PW
ID

PREPARING FOR CYBER ATTACK

Attackers try to obtain information assets in a variety of ways before launching an attack in order to gain an attack.

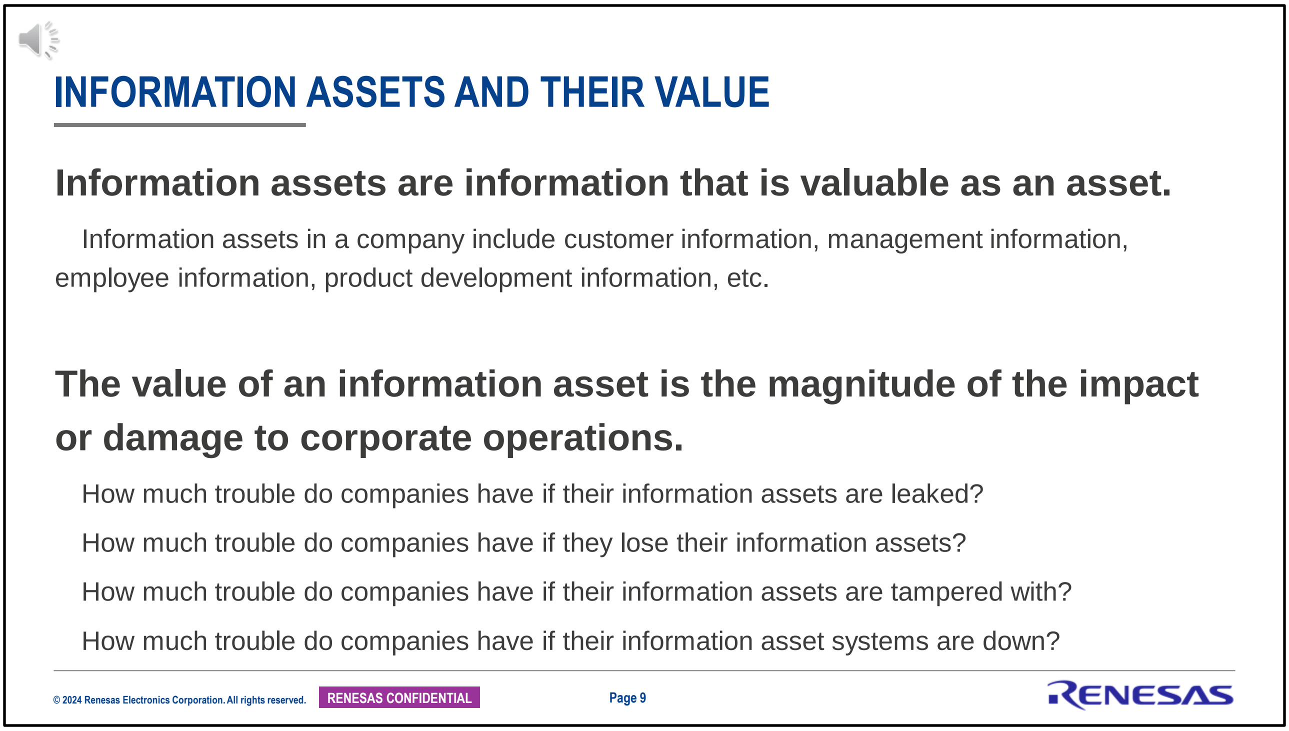
- Unauthorized access to the com
- Network eavesdropping
- Wi-Fi plagiarism
- Spyware and adware
- Negligence, loss or leakage by the parties concerned

Source: IPA Information Security 10 Major Threats

Attackers build cyberattacks from the information assets they obtain and launch attacks.

RENESAS CONFIDENTIAL RENESAS

Before launching an attack, an attacker performs an initial intrusion to obtain the information necessary to steal the desired information asset. Typical intrusion methods are listed here, and the attacker uses the information assets obtained through these methods, such as login IDs and passwords, to create a cyber attack plan against the target and launch an attack to obtain the desired information assets.



INFORMATION ASSETS AND THEIR VALUE

Information assets are information that is valuable as an asset.

Information assets in a company include customer information, management information, employee information, product development information, etc.

The value of an information asset is the magnitude of the impact or damage to corporate operations.

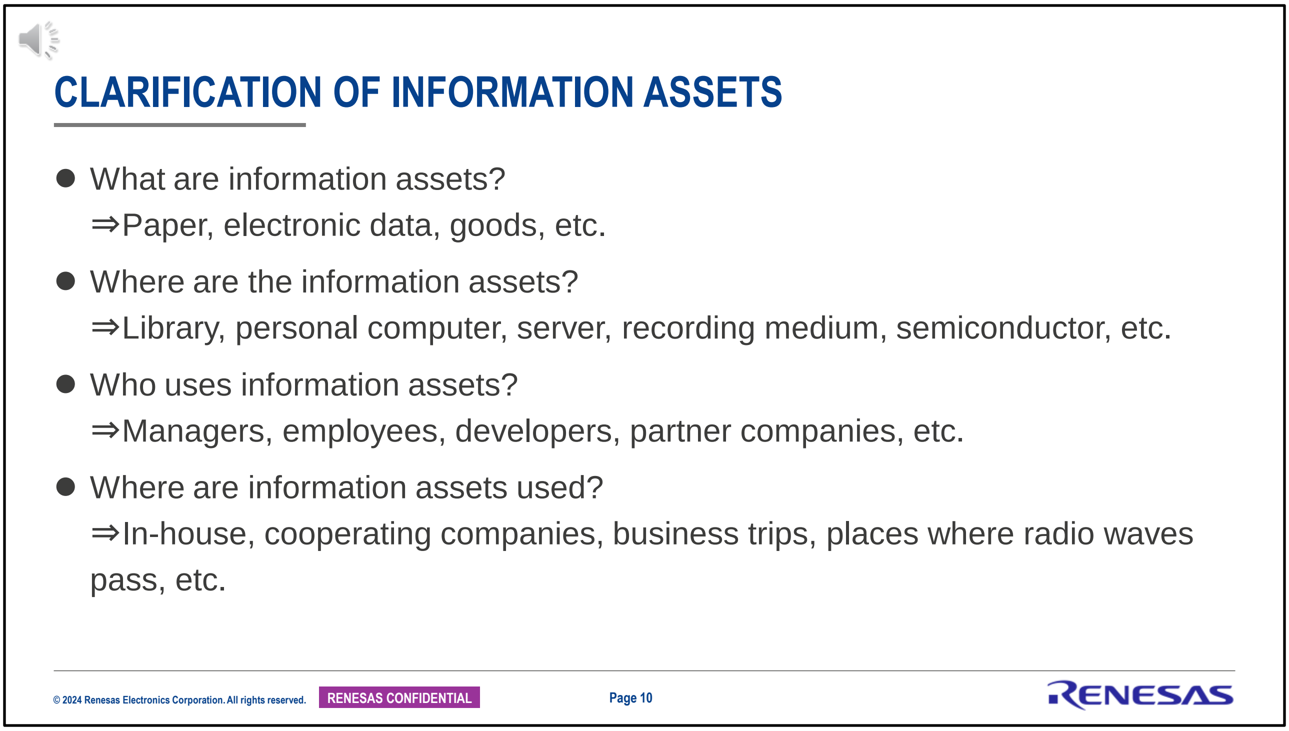
How much trouble do companies have if their information assets are leaked?

How much trouble do companies have if they lose their information assets?

How much trouble do companies have if their information assets are tampered with?

How much trouble do companies have if their information asset systems are down?

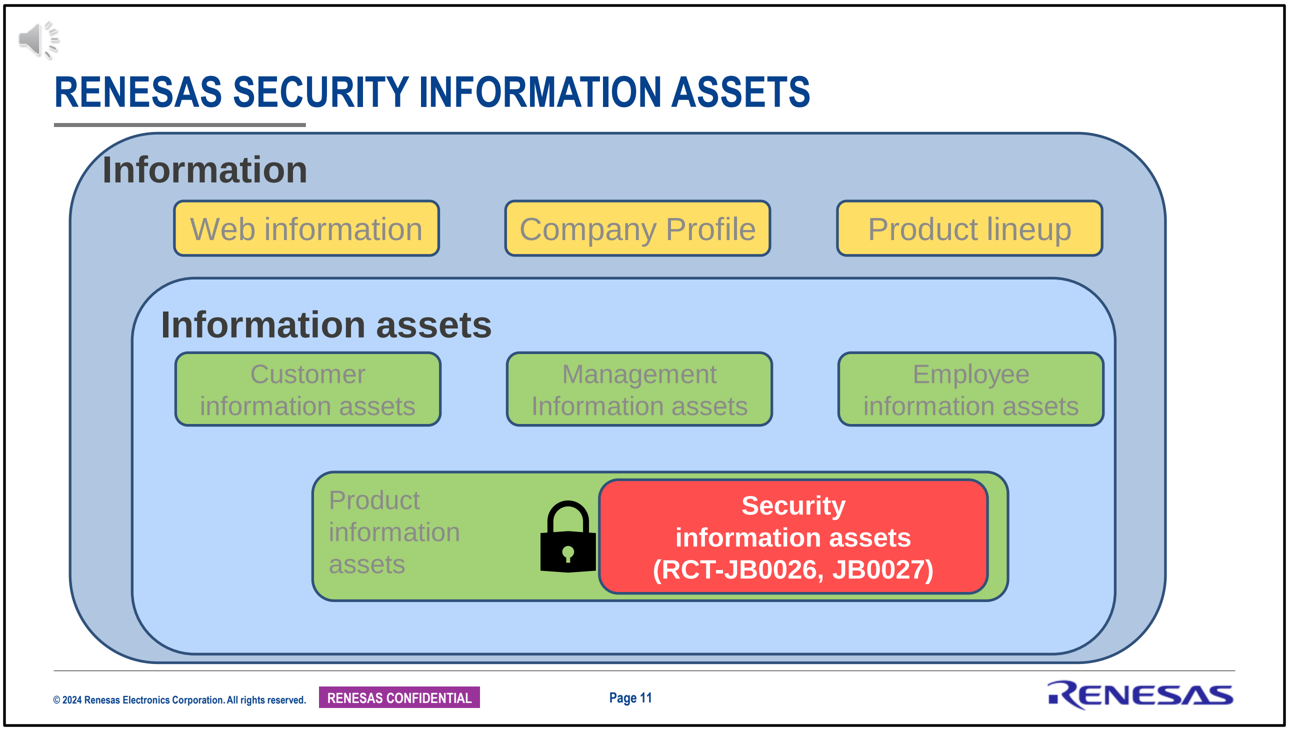
At Renesas, the information assets targeted by cyber attackers for theft include customer, management, employee, and product security information. This refers to something that creates a large positive value for the thief and a large negative impact for the stolen party. The greater the impact, the greater the value of the information asset, and the greater need for it to be protected.



CLARIFICATION OF INFORMATION ASSETS

- What are information assets?
  ⇒Paper, electronic data, goods, etc.
- Where are the information assets?
  ⇒Library, personal computer, server, recording medium, semiconductor, etc.
- Who uses information assets?
  ⇒Managers, employees, developers, partner companies, etc.
- Where are information assets used?
  ⇒In-house, cooperating companies, business trips, places where radio waves pass, etc.

Organizations with such information assets need to clarify which information assets to protect and how to protect them. For example, if the asset is paper, it is stored in a locked warehouse, and if it is electronic data, it is stored in a recording medium whose disclosure is restricted. At that time, management is performed according to the user of the information, the occasion and place where it is used. It is necessary to clarify the measures as well.



RENESAS SECURITY INFORMATION ASSETS

Information

Web information

Company Profile

Product lineup

Information assets

Customer information assets

Management Information assets

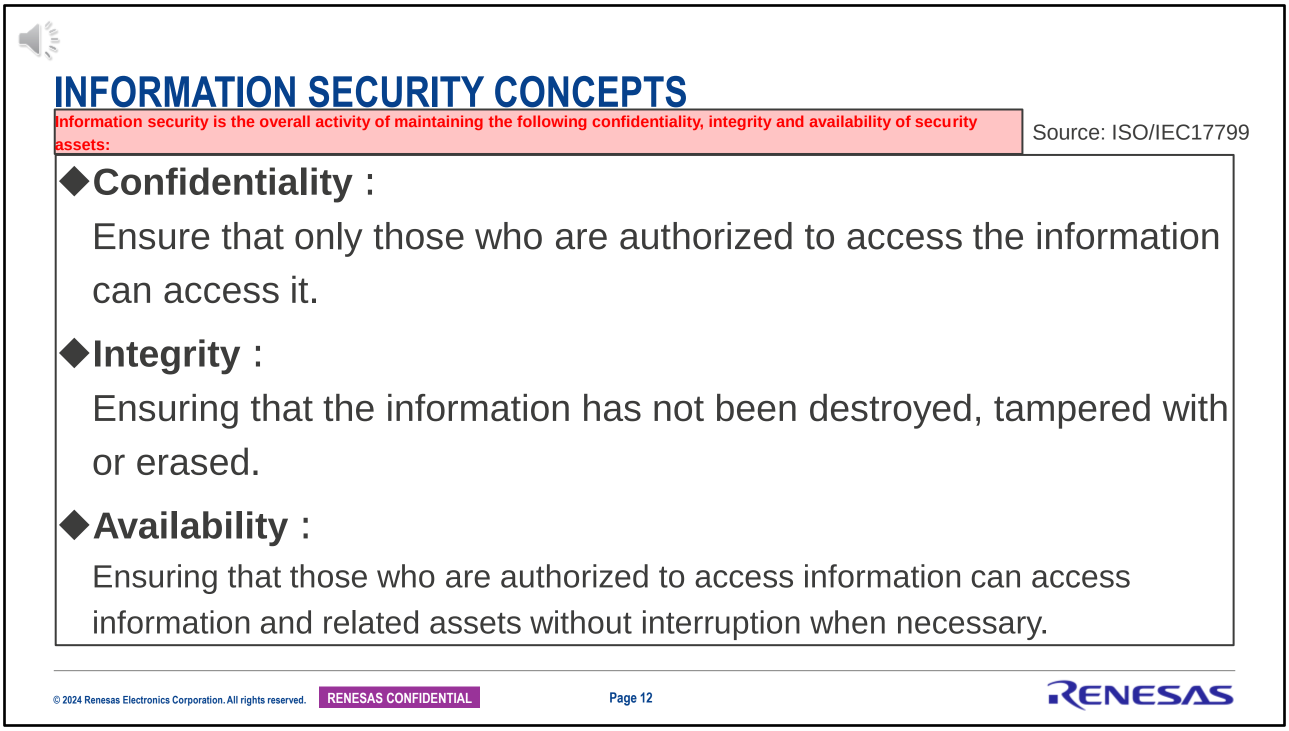
Employee information assets

Product information assets

Security information assets (RCT-JB0026, JB0027)

RENESAS CONFIDENTIAL

Based on the explanation so far, I will explain Renesas' information assets. Information assets can be divided into public information, and information assets with high security value as explained on the previous page. Among these information assets, management rules are stipulated in RCT-JB0026 and 0027 regarding the management of product-related assets, and an overview of these will be explained in Chapters 2 and 3 later.



INFORMATION SECURITY CONCEPTS

Information security is the overall activity of maintaining the following confidentiality, integrity and availability of security assets:

Source: ISO/IEC17799

◆**Confidentiality :**

Ensure that only those who are authorized to access the information can access it.

◆**Integrity :**

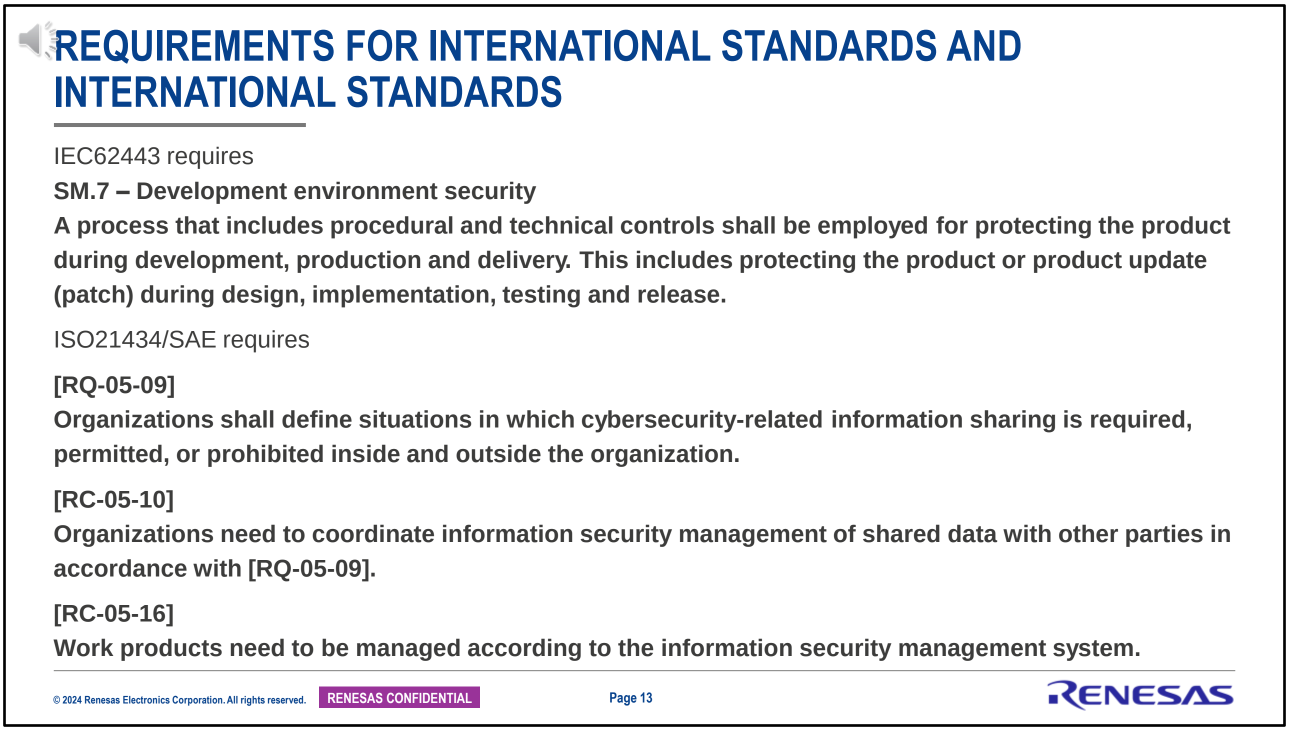
Ensuring that the information has not been destroyed, tampered with or erased.

◆**Availability :**

Ensuring that those who are authorized to access information can access information and related assets without interruption when necessary.

RENESAS CONFIDENTIAL

Security Information asset management activities are generally called as Information security, and the three basic concepts of these activities are known: confidentiality, integrity, and availability. The content is exactly as written here, but the main point is that defend strongly and correctly, but easy to use. It is also called the security C, I, and A, which are taken from the three initials.



REQUIREMENTS FOR INTERNATIONAL STANDARDS AND INTERNATIONAL STANDARDS

IEC62443 requires

SM.7 – Development environment security

A process that includes procedural and technical controls shall be employed for protecting the product during development, production and delivery. This includes protecting the product or product update (patch) during design, implementation, testing and release.

ISO21434/SAE requires

[RQ-05-09]

Organizations shall define situations in which cybersecurity-related information sharing is required, permitted, or prohibited inside and outside the organization.

[RC-05-10]

Organizations need to coordinate information security management of shared data with other parties in accordance with [RQ-05-09].

[RC-05-16]

Work products need to be managed according to the information security management system.

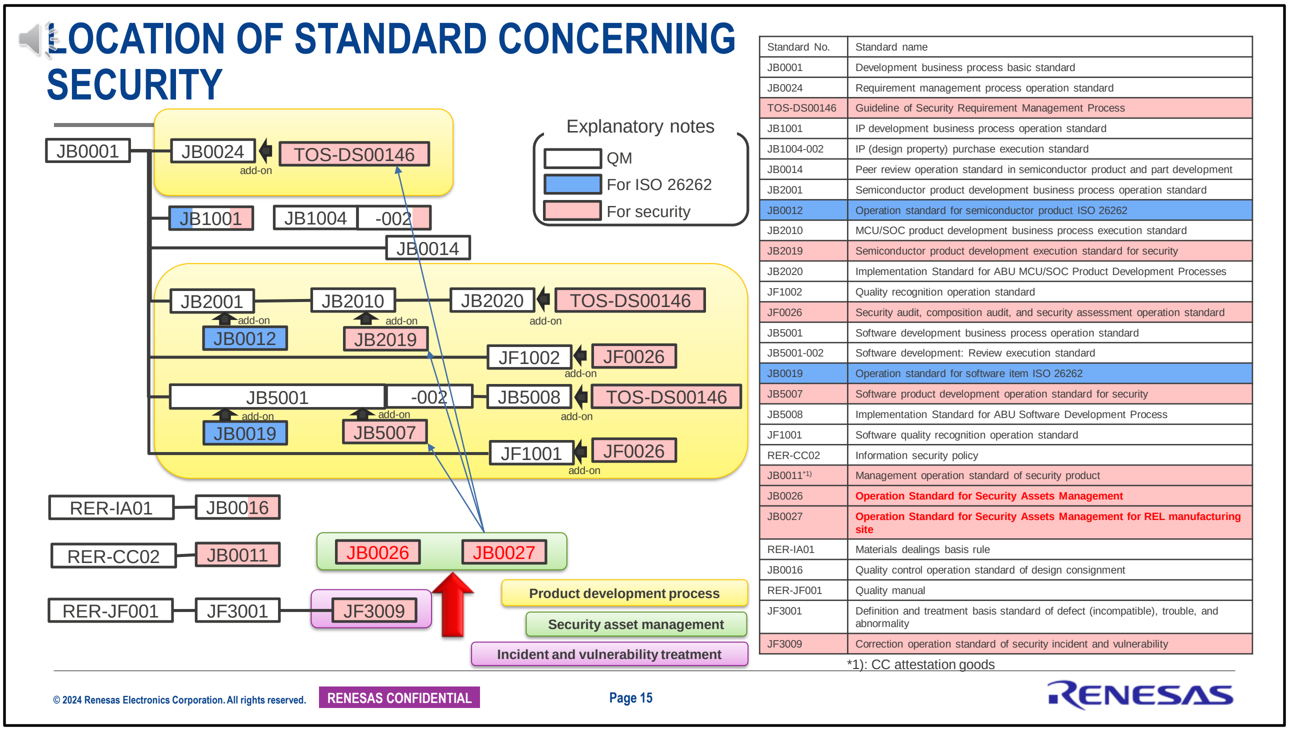
RENESAS CONFIDENTIAL Page 13

Regarding C, I, and A of security, there are requirements and recommendations in the international cybersecurity standard IEC62443 for the industrial field and the same international standard ISO/SAE21434 for the automotive field. Although not explained here, there is also a general-purpose international standard for information asset management called ISO27001, which also has regulations for C, I, and A.

2. MANAGEMENT CLASSIFICATION AND METHODS FOR SECURITY ASSETS

RENESAS CONFIDENTIAL

Chapter 2 is the implementation guidelines for security asset management.



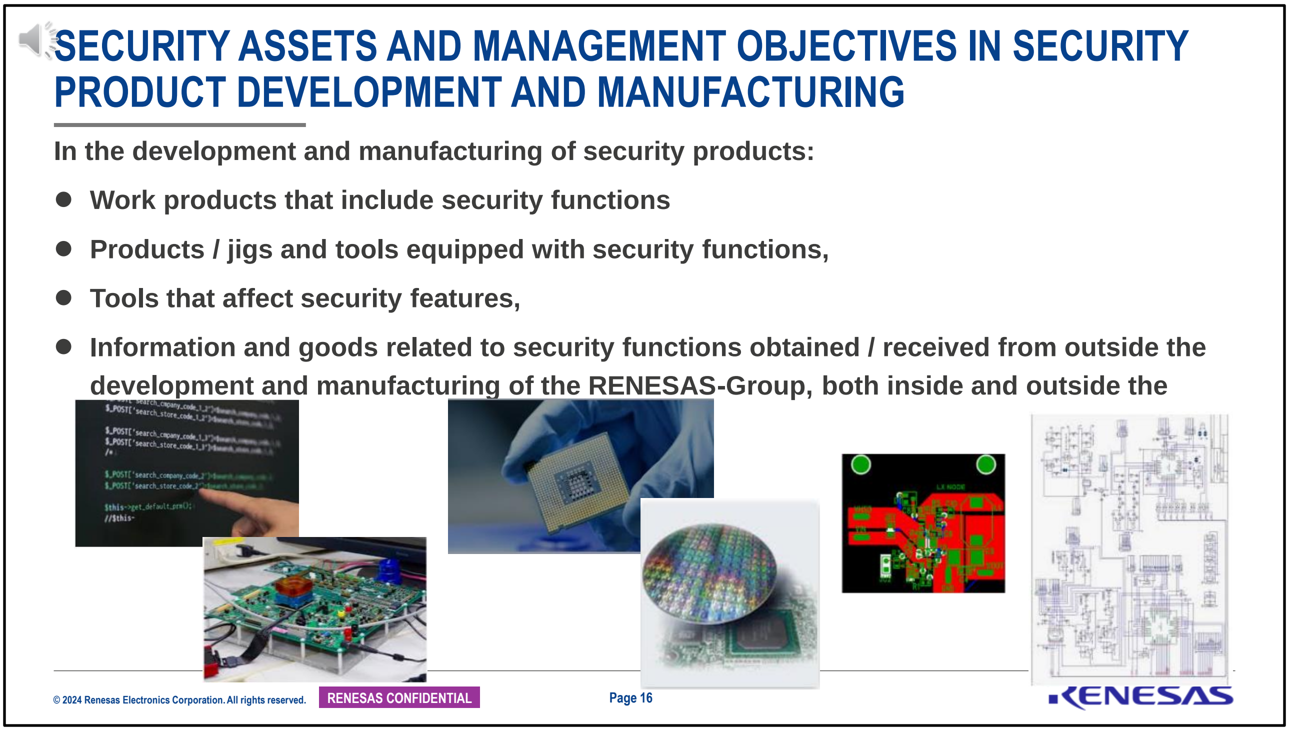
LOCATION OF STANDARD CONCERNING SECURITY

Standard No.	Standard name
JB0001	Development business process basic standard
JB0024	Requirement management process operation standard
TOS-DS00146	Guideline of Security Requirement Management Process
JB1001	IP development business process operation standard
JB1004-002	IP (design property) purchase execution standard
JB0014	Peer review operation standard in semiconductor product and part development
JB2001	Semiconductor product development business process operation standard
JB0012	Operation standard for semiconductor product ISO 26262
JB2010	MCU/SOC product development business process execution standard
JB2019	Semiconductor product development execution standard for security
JB2020	Implementation Standard for ABU MCU/SOC Product Development Processes
JF1002	Quality recognition operation standard
JF0026	Security audit, composition audit, and security assessment operation standard
JB5001	Software development business process operation standard
JB5001-002	Software development: Review execution standard
JB0019	Operation standard for software item ISO 26262
JB5007	Software product development operation standard for security
JB5008	Implementation Standard for ABU Software Development Process
JF1001	Software quality recognition operation standard
RER-CC02	Information security policy
JB0011[*1)]	Management operation standard of security product
JB0026	**Operation Standard for Security Assets Management**
JB0027	**Operation Standard for Security Assets Management for REL manufacturing site**
RER-IA01	Materials dealings basis rule
JB0016	Quality control operation standard of design consignment
RER-JF001	Quality manual
JF3001	Definition and treatment basis standard of defect (incompatible), trouble, and abnormality
JF3009	Correction operation standard of security incident and vulnerability

*1): CC attestation goods

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL Page 15

As mentioned in Chapter 1, the technical standards explained in Chapter 2 are RCT-JB0026 and 0027, and this diagram shows the position of these standards in the overall QMS. The former stipulates security information asset management rules for the development process and the latter for the manufacturing process.As shown in this diagram, these 2 standards support and complement TOS-DS00146, RCT-JB2019, and RCT-JB5007, which are technical standards related to security development.



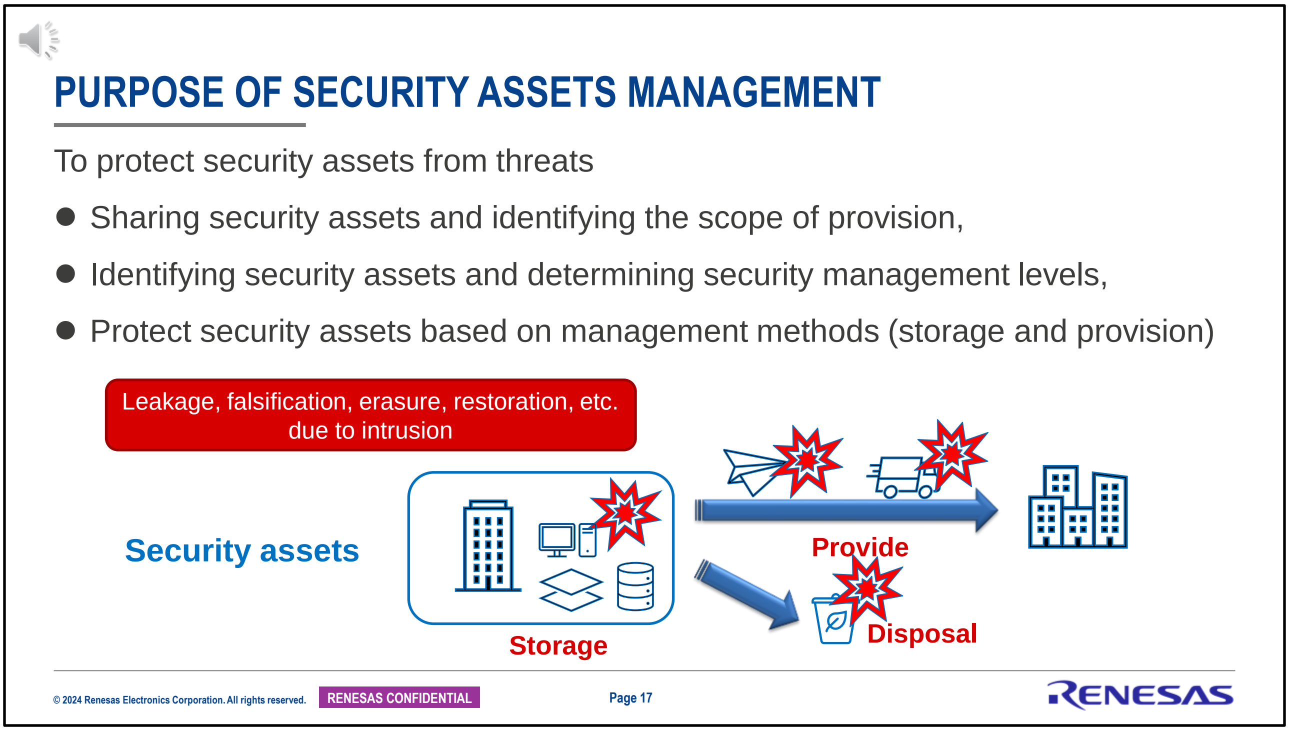
SECURITY ASSETS AND MANAGEMENT OBJECTIVES IN SECURITY PRODUCT DEVELOPMENT AND MANUFACTURING

In the development and manufacturing of security products:

- Work products that include security functions
- Products / jigs and tools equipped with security functions,
- Tools that affect security features,
- Information and goods related to security functions obtained / received from outside the development and manufacturing of the RENESAS-Group, both inside and outside the

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL Page 16

The security assets mentioned in the security-related technical standards explained on the previous page are specifically those shown here. For example, information assets generated in the security product development process include work products such as design documents and software source codes that include security functions, security function information received from outside, reticles, and security keys that are used to implement security functions. We also have jigs and tools such as evaluation boards, Test programs, etc. On the other hand, information assets generated during the manufacturing process include wafers, chips, semi-assembled products, and wasted products.



PURPOSE OF SECURITY ASSETS MANAGEMENT

To protect security assets from threats

- Sharing security assets and identifying the scope of provision,
- Identifying security assets and determining security management levels,
- Protect security assets based on management methods (storage and provision)

Leakage, falsification, erasure, restoration, etc. due to intrusion

Security assets

Storage

Provide

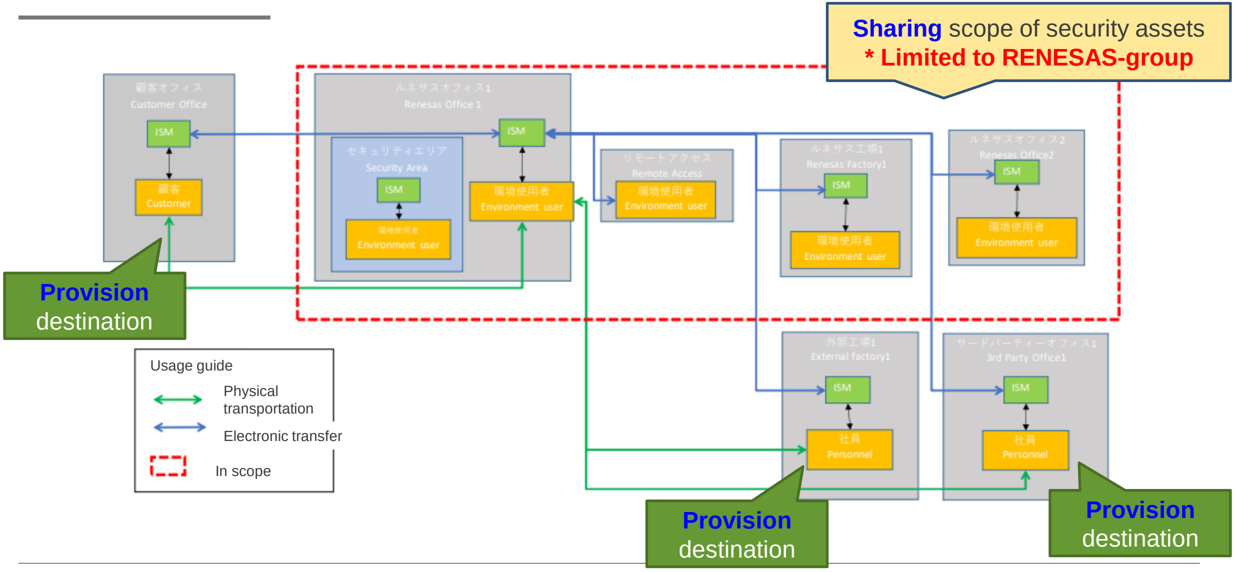
Disposal

RENESAS CONFIDENTIAL

RENESAS

I will now explain security asset management in more detail, but I will explain the purpose of asset management defined in the Renesas technical standards as a premise. In order to protect security assets from threats, it is first necessary to identify the specific security assets and then decide on the scope of information sharing and provision. Then, we assign a management level to each identified security asset, and then implement protection of the asset according to the management level based on the storage, provision, and disposal methods stipulated in the RCT. This series of activities is the purpose of security asset management.

SHARING OF SECURITY ASSETS AND IDENTIFICATION THE PROVISION SCOPE



Sharing scope of security assets
*** Limited to RENESAS-group**

Provision destination

Provision destination

Provision destination

Usage guide

↔ Physical transportation

↔ Electronic transfer

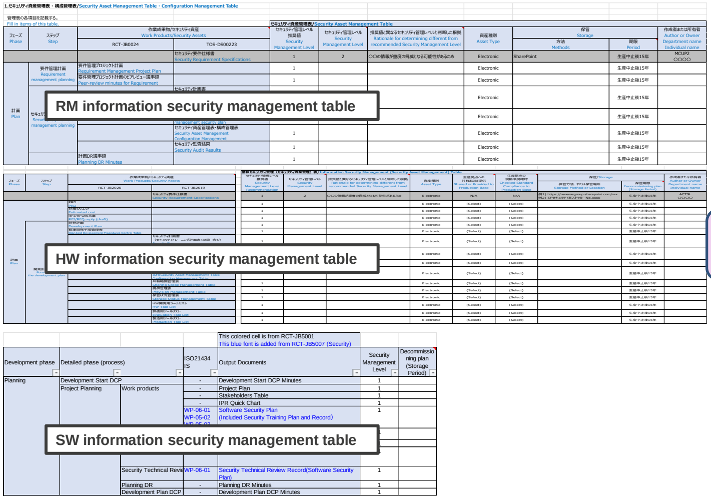
▭ In scope

RENESAS CONFIDENTIAL

First, we will explain about identifying the scope of security asset sharing and provision. The identification of sharing and provision scope is to clarify who is involved in development and production, and how to exchange security assets. For example, product development is carried out not only in the office or at home, but also at development contractors. During production after development, outsourcing companies outside the Renesas Group are involved, and customers are also involved in asset management during product sales and design-in after production. All of those are places where security assets are handled. Within this, asset management within the Renesas Group is referred to as sharing, and asset management outside of that scope is referred to as provision. This is true whether the asset is physical or electronic.

IDENTIFYING SECURITY ASSETS

The Security Asset Management Table is provided in the Security Case Creation Guide (TOS-DS00204) in the form of requirements management, semiconductor product development, and software product development.



1.セキュリティ資産管理表・構成管理表/Security Asset Management Table・Configuration Management Table

管理表の各項目を記載する。
Fill in items of this table.

セキュリティ資産管理表/Security Asset Management Table

フェーズ Phase	ステップ Step	作業成果物/セキュリティ資産 Work Products/Security Assets RCT-JB0024	作業成果物/セキュリティ資産 Work Products/Security Assets TOS-DS00223	セキュリティ管理レベル推奨値 Security Management Level	セキュリティ管理レベル Security Management Level	推奨値と異なるセキュリティ管理レベルと判断した根拠 Rationale for determining different from recommended Security Management Level	資産種別 Asset Type	保管 Storage 方法 Methods	保管 Storage 期限 Period	作成者または所有者 Author or Owner Department name Individual name
			セキュリティ要件仕様書 Security Requirement Specifications	1	2	○○の情報が重度の脅威となる可能性があるため	Electronic	SharePoint	生産中止後15年	MCUP2 ○○○○
計画 Plan	要件管理計画 Requirement management planning	要件管理プロジェクト計画 Requirement Management Project Plan		1			Electronic		生産中止後15年	
		要件管理プロジェクト計画のピアレビュー議事録 Peer-review minutes for Requirement		1			Electronic		生産中止後15年	
	セキュリ… Securi… management planning		セキュリティ計画書				Electronic		生産中止後15年	
			…management security plan				Electronic		生産中止後15年	
			セキュリティ資産管理表・構成管理表 Security Asset Management Configuration Management	1			Electronic		生産中止後15年	
			セキュリティ監査結果 Security Audit Results	1			Electronic		生産中止後15年	
		計画DR議事録 Planning DR Minutes		1			Electronic		生産中止後15年	

RM information security management table

情報セキュリティ管理（セキュリティ資産管理）表/Information Security Management (Security Asset Management) Table

フェーズ Phase	ステップ Step	作業成果物/セキュリティ資産 Work Products/Security Assets RCT-JB2020	作業成果物/セキュリティ資産 Work Products/Security Assets RCT-JB2019	セキュリティ管理レベル推奨値 Security Management Level Recommendation	セキュリティ管理レベル Security Management Level	推奨値と異なるセキュリティ管理レベルと判断した根拠 Rationale for determining different from recommended Security Management Level	資産種別 Asset Type	生産拠点への共有または提供 Shared or Provided to Production Base	生産拠点の規格準拠確認 Checked Standard Compliance to Production Base	保管/Storage 保管方法、または保管場所 Storage Method or Location	保管/Storage 保管期限 Decommissioning plan (Storage Period)	作成者または所有者 Author or Owner Department name Individual name
			セキュリティ要件仕様書 Security Requirement Specifications	1	2	○○の情報が重度の脅威となる可能性があるため	Electronic	N/A	N/A	例1) https://renesasgroup.sharepoint.com/xxx 例2) SFセキュリティ室ストッカーNo.xxxx	生産中止後15年	ACTSL ○○○○
計画 Plan		PRD PRD		1			Electronic	(Select)	(Select)		生産中止後15年	
		見積もりコスト Estimated cost		1			Electronic	(Select)	(Select)		生産中止後15年	
		RFI/RFQ回答案 RFI/RFQ reply (draft)		1			Electronic	(Select)	(Select)		生産中止後15年	
	開発計… Form… the development plan	開発計画 Development Plan		1			Electronic	(Select)	(Select)		生産中止後15年	
		標準開発手順管理表 Standard Development Procedures Control Table		1			Electronic	(Select)	(Select)		生産中止後15年	
			セキュリティ計画書（セキュリティトレーニング計画書/記録 含む） Security Plan	1			Electronic	(Select)	(Select)		生産中止後15年	
							Electronic	(Select)	(Select)		生産中止後15年	
							Electronic	(Select)	(Select)		生産中止後15年	
			ISM(Security Asset Management) Table Configuration Management Table				Electronic	(Select)	(Select)		生産中止後15年	
			共有範囲管理表 Sharing Scope Management Table	1			Electronic	(Select)	(Select)		生産中止後15年	
			提供管理表 Provision Management Table	1			Electronic	(Select)	(Select)		生産中止後15年	
			保管状況管理表 Storage Status Management Table	1			Electronic	(Select)	(Select)		生産中止後15年	
			HW開発用ツールリスト HW Tool List	1			Electronic	(Select)	(Select)		生産中止後15年	
			評価用ツールリスト Evaluation Tool List	1			Electronic	(Select)	(Select)		生産中止後15年	
			製造用ツールリスト Production Tool List	1			Electronic	(Select)	(Select)		生産中止後15年	

HW information security management table

This colored cell is from RCT-JB5001
This blue font is added from RCT-JB5007 (Security)

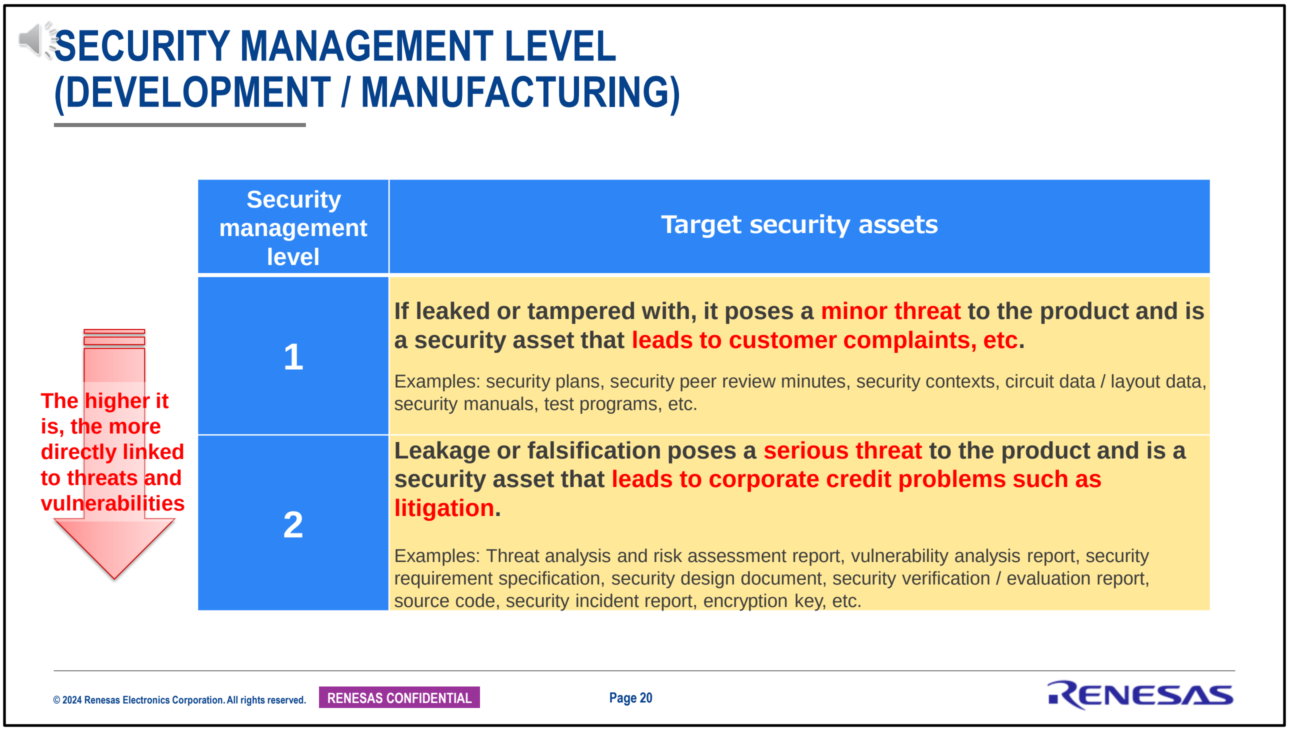
Development phase	Detailed phase (process)		ISO21434 IS	Output Documents	Security Management Level	Decommissioning plan (Storage Period)
Planning	Development Start DCP		-	Development Start DCP Minutes	1	
	Project Planning	Work products	-	Project Plan	1	
			-	Stakeholders Table	1	
			-	IPR Quick Chart	1	
			WP-06-01 WP-05-02	Software Security Plan (Included Security Training Plan and Record)	1	
		Security Technical Revie	WP-06-01	Security Technical Review Record(Software Security Plan)	1	
		Planning DR	-	Planning DR Minutes	1	
		Development Plan DCP	-	Development Plan DCP Minutes	1	

SW information security management table

In semiconductor product development, the asset list is transmitted from the development department to the production base after the development start DCP is completed.

RENESAS CONFIDENTIAL

Let's start explanation from identifying security assets. Renesas has incorporated asset management table into the security case specified by ISO/SAE21434. Asset deliverables and security management levels are determined through the creation of initial security cases in each planning phase of requirements management, semiconductor product development, and software product development. In semiconductor product development, the development department transmits the asset information necessary for the production process to the manufacturing department, and the manufacturing department takes steps to manage security assets using an asset management plan based on that information and the requirements of RCT-JB0027.



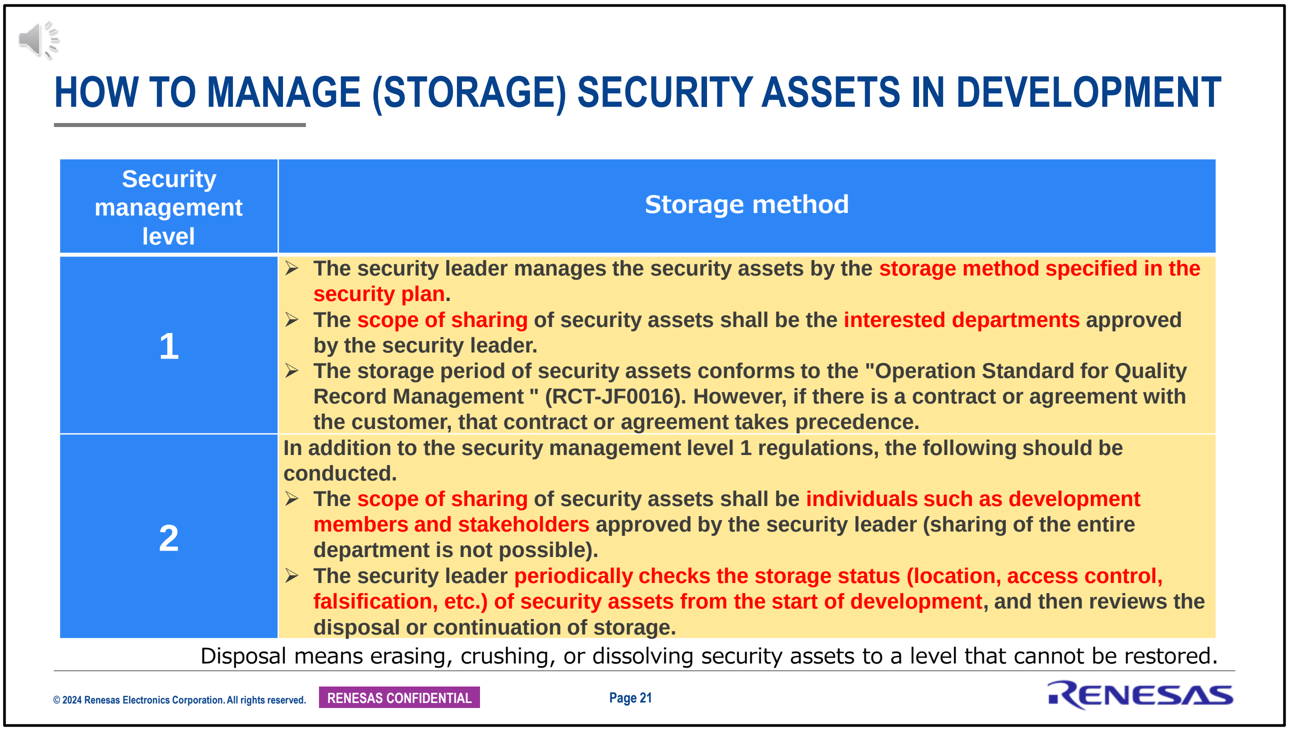
SECURITY MANAGEMENT LEVEL (DEVELOPMENT / MANUFACTURING)

The higher it is, the more directly linked to threats and vulnerabilities

Security management level	Target security assets
1	**If leaked or tampered with, it poses a minor threat to the product and is a security asset that leads to customer complaints, etc.** Examples: security plans, security peer review minutes, security contexts, circuit data / layout data, security manuals, test programs, etc.
2	**Leakage or falsification poses a serious threat to the product and is a security asset that leads to corporate credit problems such as litigation.** Examples: Threat analysis and risk assessment report, vulnerability analysis report, security requirement specification, security design document, security verification / evaluation report, source code, security incident report, encryption key, etc.

RENESAS CONFIDENTIAL

Next, we will explain how to assign security management levels. Security management levels are divided into 1 and 2, depending on the degree of impact that leakage or tampering of information assets would have on the product, with 2 having stricter management. Level 1 is assigned to assets whose leakage or tampering poses only a minor threat and would result in a customer complaint at best, while Level 2 is assigned to assets that pose a severe threat and could lead to litigation or other problems with the company's credibility.



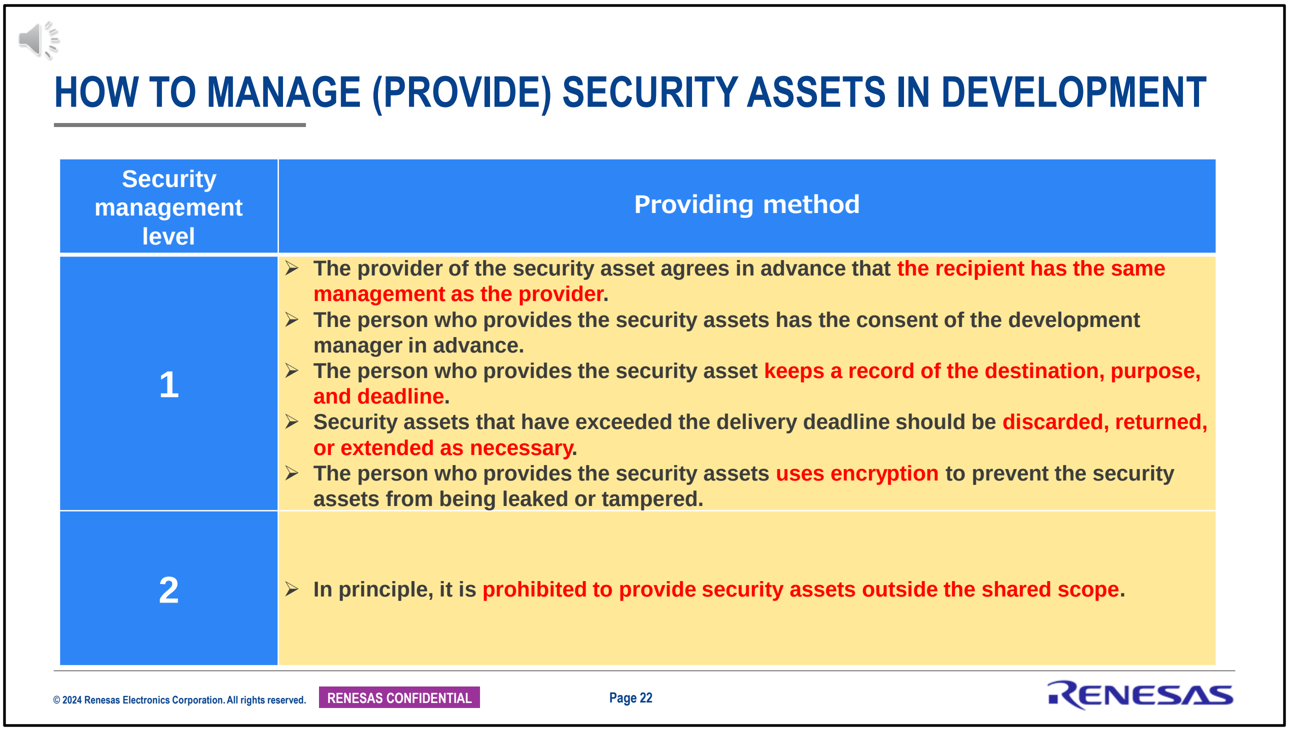
HOW TO MANAGE (STORAGE) SECURITY ASSETS IN DEVELOPMENT

Security management level	Storage method
1	➢ The security leader manages the security assets by the **storage method specified in the security plan**. ➢ The **scope of sharing** of security assets shall be the **interested departments** approved by the security leader. ➢ The storage period of security assets conforms to the "Operation Standard for Quality Record Management " (RCT-JF0016). However, if there is a contract or agreement with the customer, that contract or agreement takes precedence.
2	In addition to the security management level 1 regulations, the following should be conducted. ➢ The **scope of sharing** of security assets shall be **individuals such as development members and stakeholders** approved by the security leader (sharing of the entire department is not possible). ➢ The security leader **periodically checks the storage status (location, access control, falsification, etc.) of security assets from the start of development**, and then reviews the disposal or continuation of storage.

Disposal means erasing, crushing, or dissolving security assets to a level that cannot be restored.

RENESAS CONFIDENTIAL

From here on, this slide and the next slide will explain the differences in storage and provision methods for each security management level in development stipulated in RCT-JB0026. First, let's talk about how to store assets during development. Sharing of assets at management level 1 is permitted only to interested departments within Renesas by the security leader at the department level during security planning, whereas at level 2, sharing by department is not permitted even within Renesas, and sharing by individual personel is only allowed. In addition, security leaders are required to regularly check the status of asset storage. Confirmation of storage status involves confirming that assets are stored where they should be, that access controls do not exceed specified limits, and that there is no evidence of asset tampering. Regardless of the management level, the storage period of security assets is determined according to the quality record management operational standard RCT-JF0016, and it is necessary to decide whether to discard or continue storage at the time of this confirmation, but if there is a contract or agreement with a specific customer,it takes priority. When disposing of assets, it is mandatory to crush them to the point where they cannot be restored, regardless of the level, and then dispose of them.



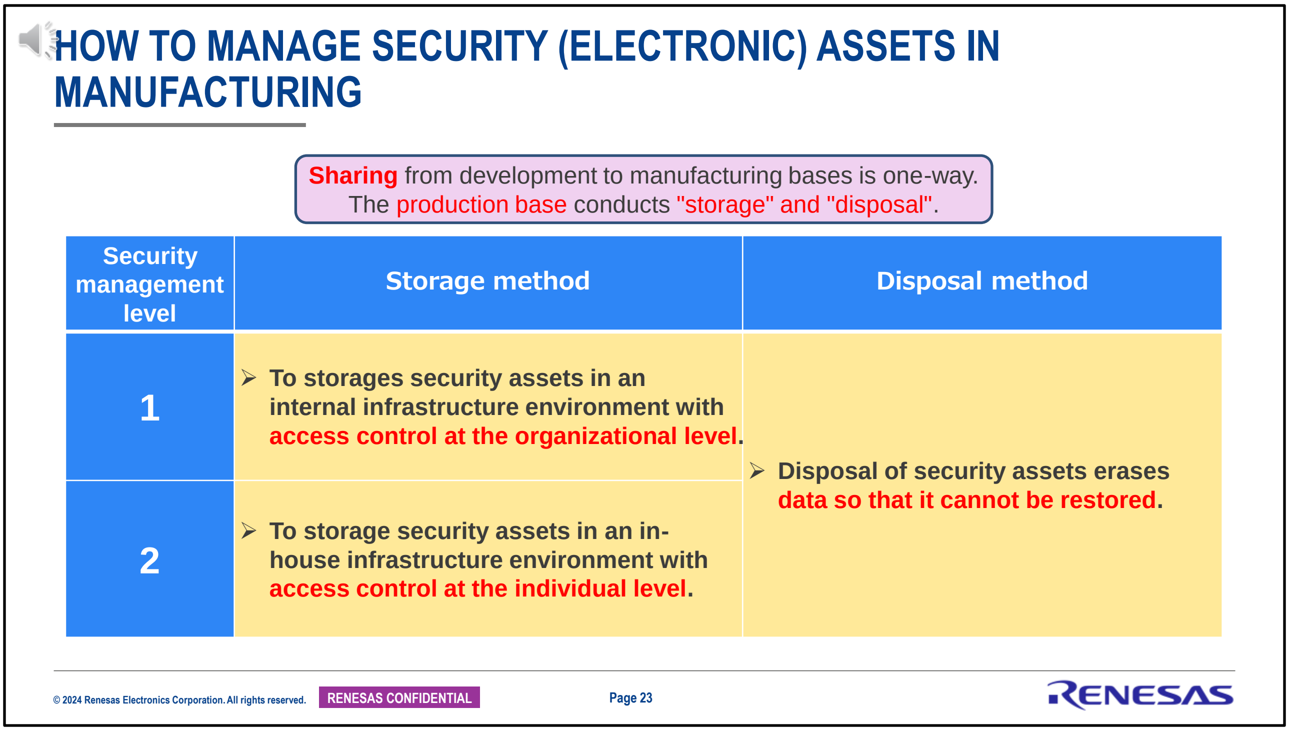
HOW TO MANAGE (PROVIDE) SECURITY ASSETS IN DEVELOPMENT

Security management level	Providing method
1	➢ The provider of the security asset agrees in advance that **the recipient has the same management as the provider**. ➢ The person who provides the security assets has the consent of the development manager in advance. ➢ The person who provides the security asset **keeps a record of the destination, purpose, and deadline**. ➢ Security assets that have exceeded the delivery deadline should be **discarded, returned, or extended as necessary**. ➢ The person who provides the security assets **uses encryption** to prevent the security assets from being leaked or tampered.
2	➢ In principle, it is **prohibited to provide security assets outside the shared scope**.

RENESAS CONFIDENTIAL

RENESAS

Next, we will explain how to provide assets during development. First, regarding security management level 1, we agree in advance that the receiver will manage the provided security assets in the same manner as the provider. Then we provide the assets after taking measures against leakage and tampering, such as encryption, and keep a record of the provision. Security assets that have exceeded the delivery deadline will be disposed of or returned to the provider, or the deadline will be extended as necessary. Next is security management level 2 assets are principally totally prohibited from being provided to outside of the shared scope. This rule was set in consideration of the magnitude of the impact caused by the leakage of Level 2 assets.



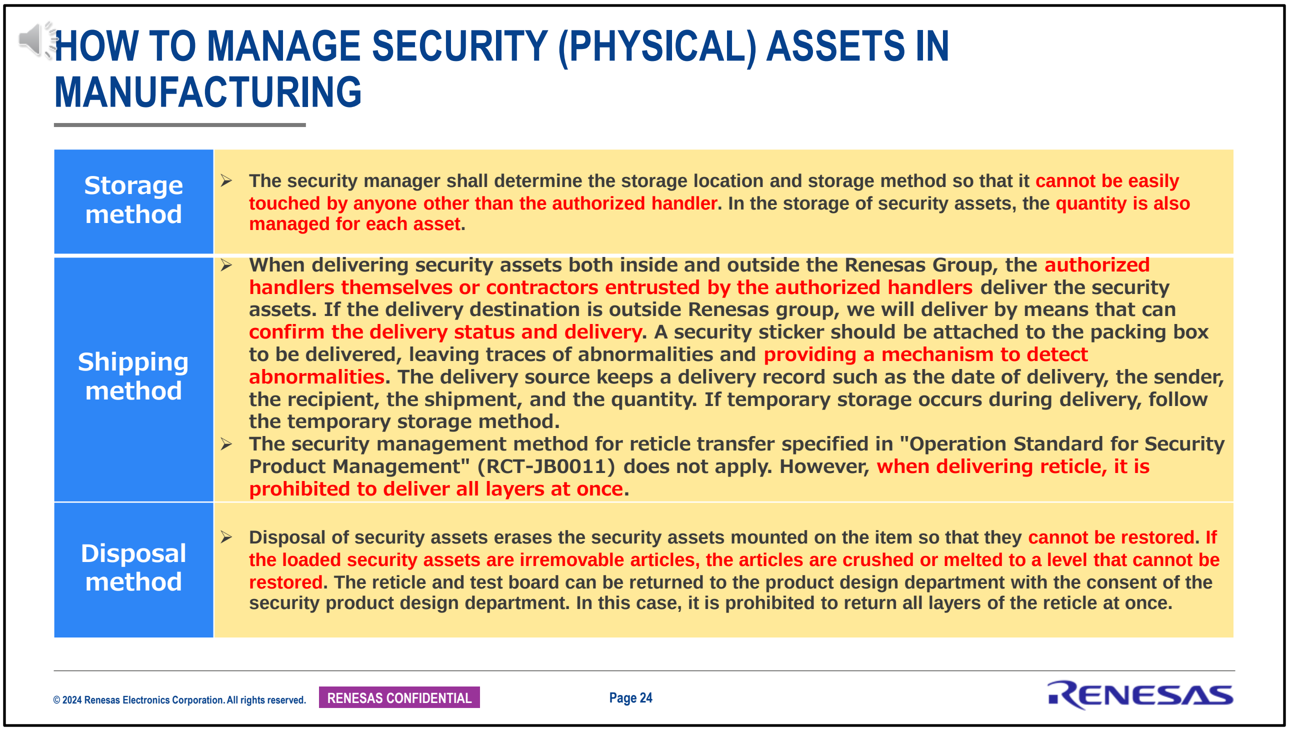
HOW TO MANAGE SECURITY (ELECTRONIC) ASSETS IN MANUFACTURING

Sharing from development to manufacturing bases is one-way.
The production base conducts "storage" and "disposal".

Security management level	Storage method	Disposal method
1	➢ To storages security assets in an internal infrastructure environment with access control at the organizational level.	➢ Disposal of security assets erases data so that it cannot be restored.
2	➢ To storage security assets in an in-house infrastructure environment with access control at the individual level.	

RENESAS CONFIDENTIAL

Next, in this slide and the next slide, we will explain the differences in storage, provision, and disposal methods for each security management level in production stipulated in RCT-JB0027. In production, there is only unilateral sharing from development to production factories. There is no provision and production factories only store and dispose of the given assets.
First, we will explain how to store and dispose of electronic assets during production. The difference between levels 1 and 2 regarding storage is the same as the storage in development explained earlier, with level 1 providing access control on a department-by-department basis and level 2 on an individual-by-individual basis. On the other hand, the same applies to disposal; there is no difference depending on the level, and both require pulverization and disposal to prevent data recovery.



HOW TO MANAGE SECURITY (PHYSICAL) ASSETS IN MANUFACTURING

Storage method	➢ The security manager shall determine the storage location and storage method so that it cannot be easily touched by anyone other than the authorized handler. In the storage of security assets, the quantity is also managed for each asset.
Shipping method	➢ When delivering security assets both inside and outside the Renesas Group, the authorized handlers themselves or contractors entrusted by the authorized handlers deliver the security assets. If the delivery destination is outside Renesas group, we will deliver by means that can confirm the delivery status and delivery. A security sticker should be attached to the packing box to be delivered, leaving traces of abnormalities and providing a mechanism to detect abnormalities. The delivery source keeps a delivery record such as the date of delivery, the sender, the recipient, the shipment, and the quantity. If temporary storage occurs during delivery, follow the temporary storage method. ➢ The security management method for reticle transfer specified in "Operation Standard for Security Product Management" (RCT-JB0011) does not apply. However, when delivering reticle, it is prohibited to deliver all layers at once.
Disposal method	➢ Disposal of security assets erases the security assets mounted on the item so that they cannot be restored. If the loaded security assets are irremovable articles, the articles are crushed or melted to a level that cannot be restored. The reticle and test board can be returned to the product design department with the consent of the security product design department. In this case, it is prohibited to return all layers of the reticle at once.

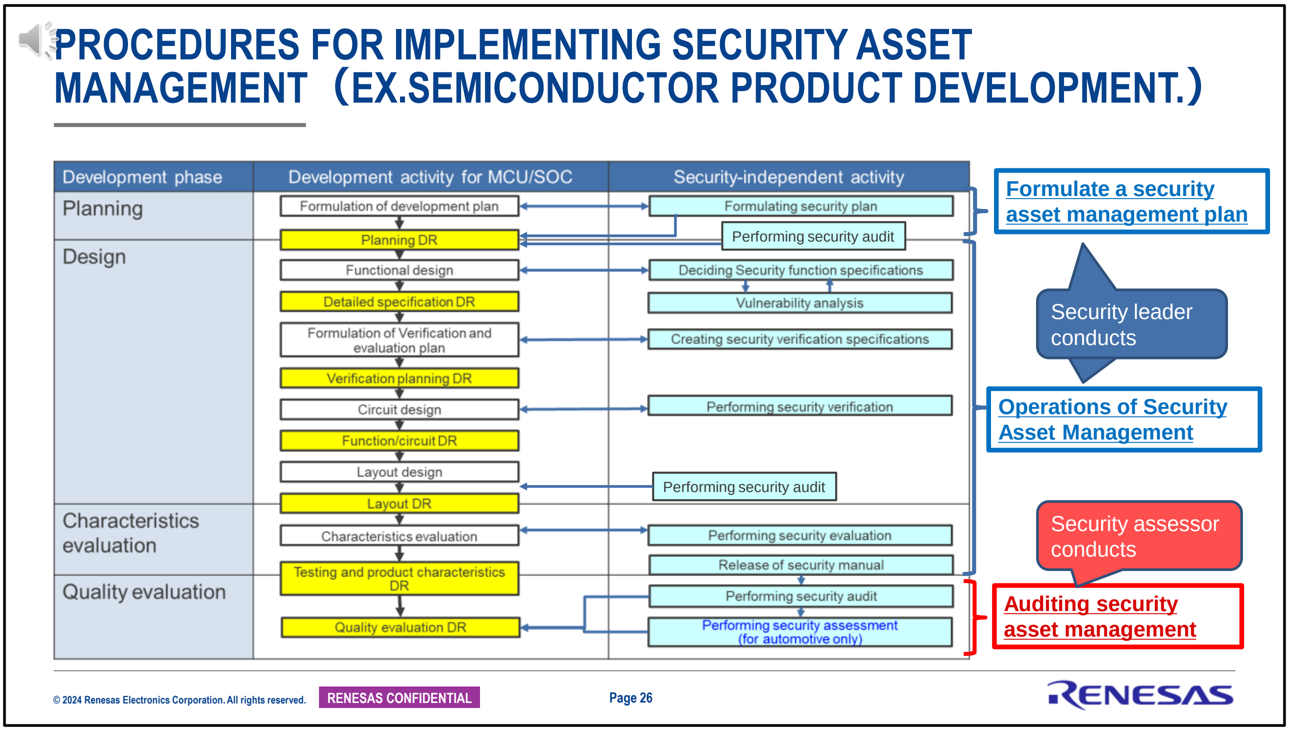
RENESAS CONFIDENTIAL

Next, we will explain how to store and dispose of physical assets during production, but there is no difference between Level 1 and Level 2. As for the storage method, the security manager should determine the storage location and method, and the storage should be managed in a place where it cannot be easily accessed by anyone other than authorized handlers, and the quantity of assets should also be subject to management. That is what is required. Regarding delivery methods, whether within or outside the Renesas Group, when delivering security assets, it is stipulated that the security assets must be delivered by the authorized handler himself or by a company entrusted by the authorized handler. If the delivery destination is outside our group, please use a method that allows you to confirm the delivery status and delivery, keep a record of the delivery, and place a security seal on the packaging box before shipping to prevent any abnormalities. There is a need for devices to leave behind traces. In particular, when it comes to receiving and receiving reticles, shipping all-layer reticles at once is prohibited due to the risk of reverse engineering due to theft. Finally, regarding the disposal method, as with electronic assets, it is required to crush them so that they cannot be restored before disposing of them.

3. SECURITY ASSET MANAGEMENT PROCEDURES

RENESAS CONFIDENTIAL

Chapter 3 is the procedure for security asset management.



PROCEDURES FOR IMPLEMENTING SECURITY ASSET MANAGEMENT （EX.SEMICONDUCTOR PRODUCT DEVELOPMENT.）

Development phase	Development activity for MCU/SOC	Security-independent activity
Planning	Formulation of development plan	Formulating security plan
	Planning DR	Performing security audit
Design	Functional design	Deciding Security function specifications
	Detailed specification DR	Vulnerability analysis
	Formulation of Verification and evaluation plan	Creating security verification specifications
	Verification planning DR	
	Circuit design	Performing security verification
	Function/circuit DR	
	Layout design	Performing security audit
	Layout DR	
Characteristics evaluation	Characteristics evaluation	Performing security evaluation
	Testing and product characteristics DR	Release of security manual
Quality evaluation		Performing security audit
	Quality evaluation DR	Performing security assessment (for automotive only)

Formulate a security asset management plan

Security leader conducts

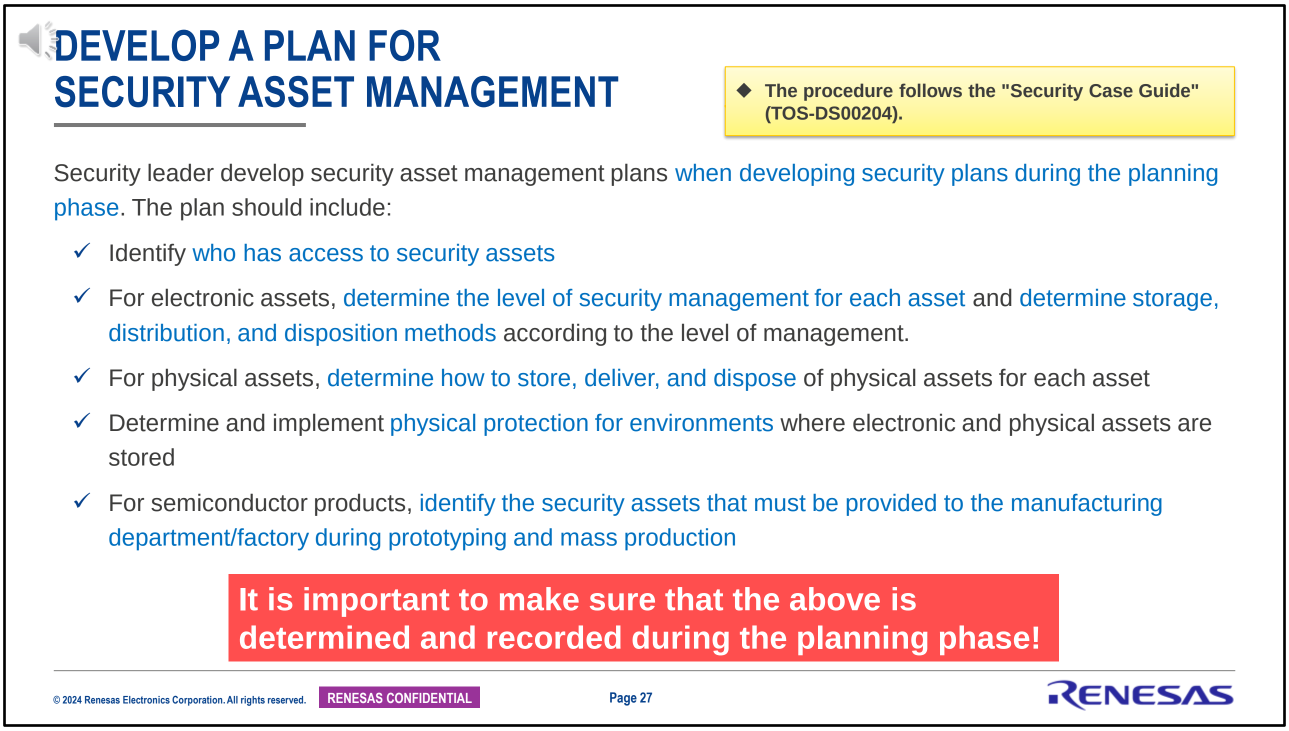
Operations of Security Asset Management

Security assessor conducts

Auditing security asset management

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL Page 26

We will explain security asset management procedures using an example of semiconductor product development milestones specified in RCT-JB2019. The flow of this slide shows the main design activities in security product development and the security management that follows them. First, a security plan is created in the planning phase, and a security asset management plan is also created as part of that plan. Then, a security assessor conducts a third-party assessment of the security assets output from the design activities to determine whether the security asset management has been performed correctly based on the asset management plan. This chart has been simplified so that the assessment is performed only once during the quality evaluation phase, but in reality, the assessment is performed several times during development time to time.



DEVELOP A PLAN FOR SECURITY ASSET MANAGEMENT

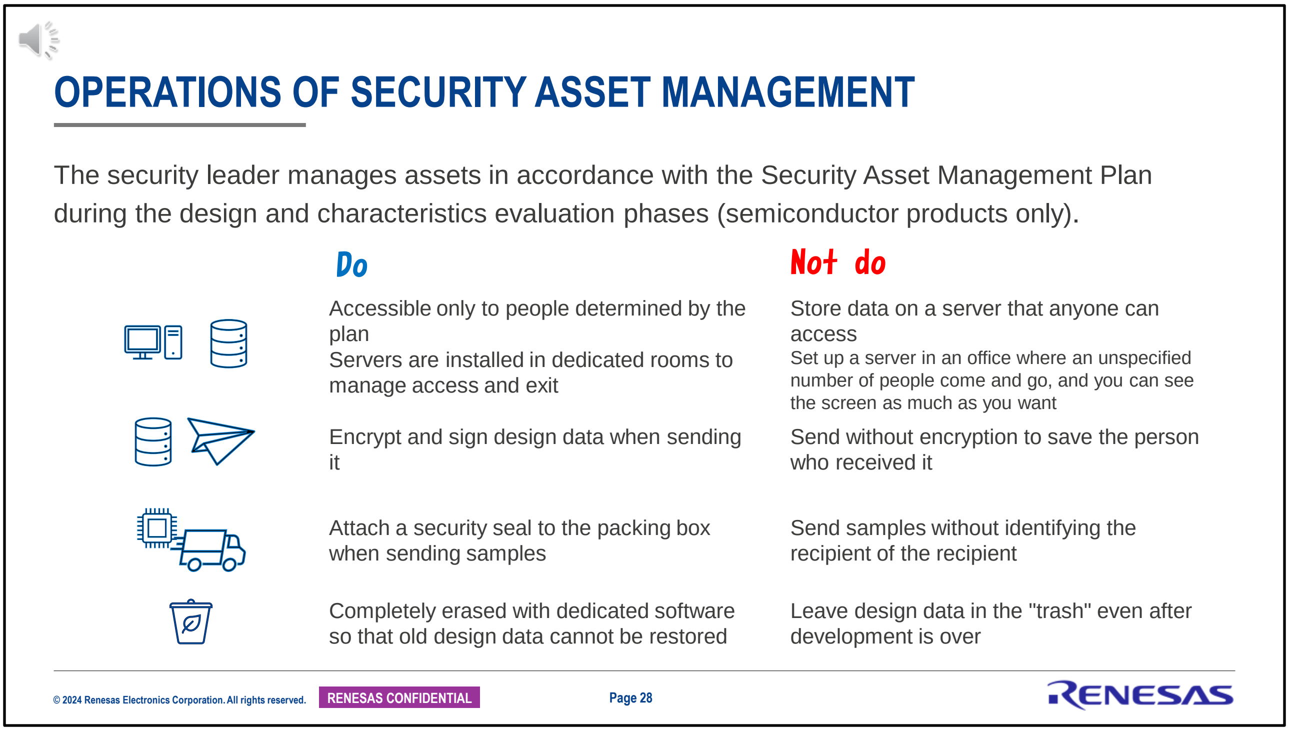
◆ The procedure follows the "Security Case Guide" (TOS-DS00204).

Security leader develop security asset management plans when developing security plans during the planning phase. The plan should include:

- ✓ Identify who has access to security assets
- ✓ For electronic assets, determine the level of security management for each asset and determine storage, distribution, and disposition methods according to the level of management.
- ✓ For physical assets, determine how to store, deliver, and dispose of physical assets for each asset
- ✓ Determine and implement physical protection for environments where electronic and physical assets are stored
- ✓ For semiconductor products, identify the security assets that must be provided to the manufacturing department/factory during prototyping and mass production

It is important to make sure that the above is determined and recorded during the planning phase!

As I mentioned in the previous slide, I would like to explain about developing a security asset management plan. When security leaders develop a security plan during the planning phase, they must also develop a plan for security asset management. There are five things that should be included in a security asset management plan, but they are all included in the template specified in TOS-DS00204, and basically an asset management plan is completed by completing the corresponding template. Note that EPSG provides a different template from HPCSG in the Security Asset Management and Configuration Management Guide for Industrial and Consumer Product Development, TOS-DS00231, but the concept for asset management plans is the same.



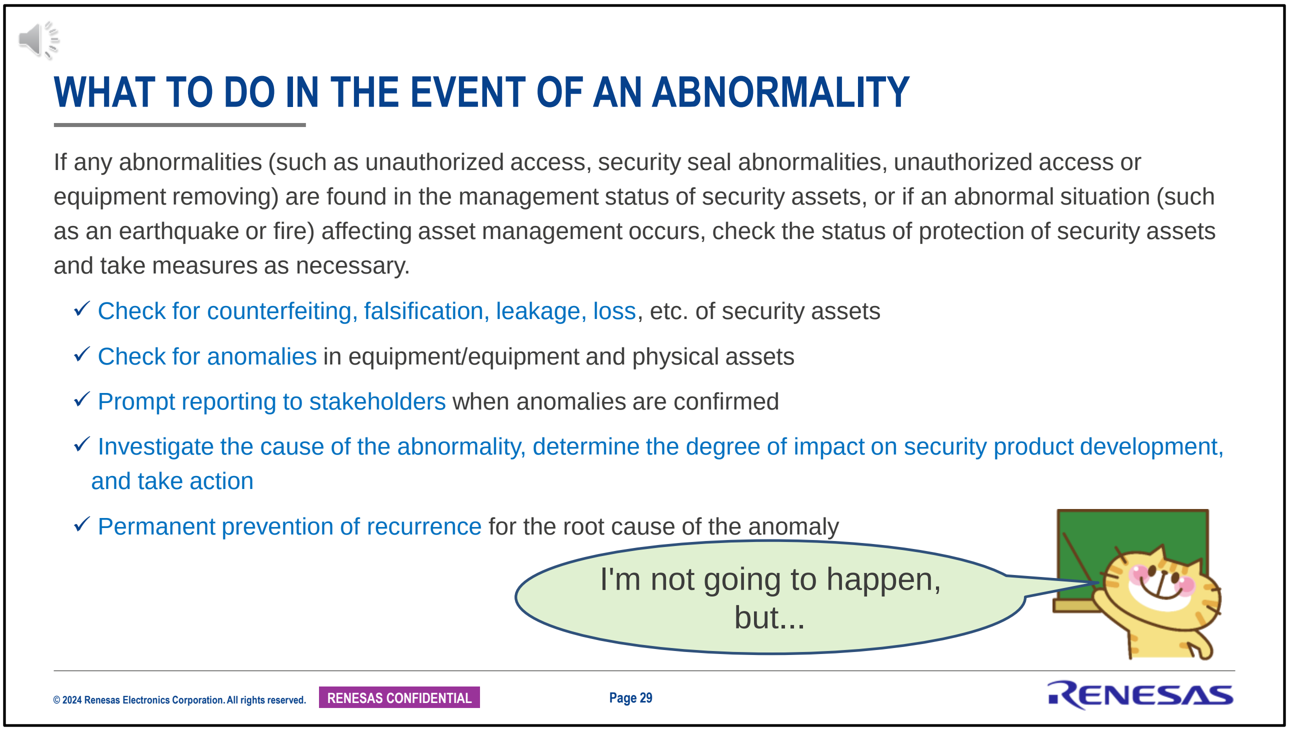
OPERATIONS OF SECURITY ASSET MANAGEMENT

The security leader manages assets in accordance with the Security Asset Management Plan during the design and characteristics evaluation phases (semiconductor products only).

Do	Not do
Accessible only to people determined by the plan Servers are installed in dedicated rooms to manage access and exit	Store data on a server that anyone can access Set up a server in an office where an unspecified number of people come and go, and you can see the screen as much as you want
Encrypt and sign design data when sending it	Send without encryption to save the person who received it
Attach a security seal to the packing box when sending samples	Send samples without identifying the recipient of the recipient
Completely erased with dedicated software so that old design data cannot be restored	Leave design data in the "trash" even after development is over

RENESAS CONFIDENTIAL

Once an asset management plan has been formulated, actual management operations will be carried out in accordance with the plan during development phase and manufacturing phase.
This slide is just an example of what you should do and should not do when complying with the management plan.



WHAT TO DO IN THE EVENT OF AN ABNORMALITY

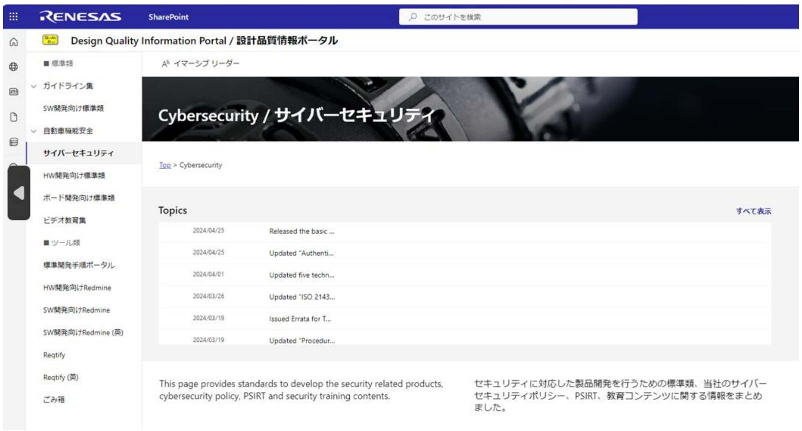
If any abnormalities (such as unauthorized access, security seal abnormalities, unauthorized access or equipment removing) are found in the management status of security assets, or if an abnormal situation (such as an earthquake or fire) affecting asset management occurs, check the status of protection of security assets and take measures as necessary.

- ✓ Check for counterfeiting, falsification, leakage, loss, etc. of security assets
- ✓ Check for anomalies in equipment/equipment and physical assets
- ✓ Prompt reporting to stakeholders when anomalies are confirmed
- ✓ Investigate the cause of the abnormality, determine the degree of impact on security product development, and take action
- ✓ Permanent prevention of recurrence for the root cause of the anomaly

RENESAS CONFIDENTIAL

At the end of this chapter, we will explain what to do when an abnormality occurs in security assets. In the unlikely event that some kind of abnormality is found in the management status of security assets, such as unauthorized access, traces of peeled-off security seals, unauthorized entry/exit records, etc., check the protection status of security assets and take necessary measures are needed. Check to see if security assets have been counterfeited, tampered with, leaked or lost, and if an abnormality is detected, promptly report to stakeholders, investigate the cause, and determine the degree of impact on security products. Those series of activities must be carried out together with stakeholders such as the PSIRT and security leaders, including making decisions, taking actions based on the decisions, and implementing permanent measures to prevent recurrence. For details, please refer to the explanation regarding security incidents in Education Module C.

“SECURITY RELATED STANDARD” SITE



Topics

2024/04/25	Released the basic ...
2024/04/25	Updated "Authenti...
2024/04/01	Updated five techn...
2024/03/26	Updated "ISO 2143...
2024/03/19	Issued Errata for T...
2024/03/19	Updated "Procedur...

This page provides standards to develop the security related products, cybersecurity policy, PSIRT and security training contents.

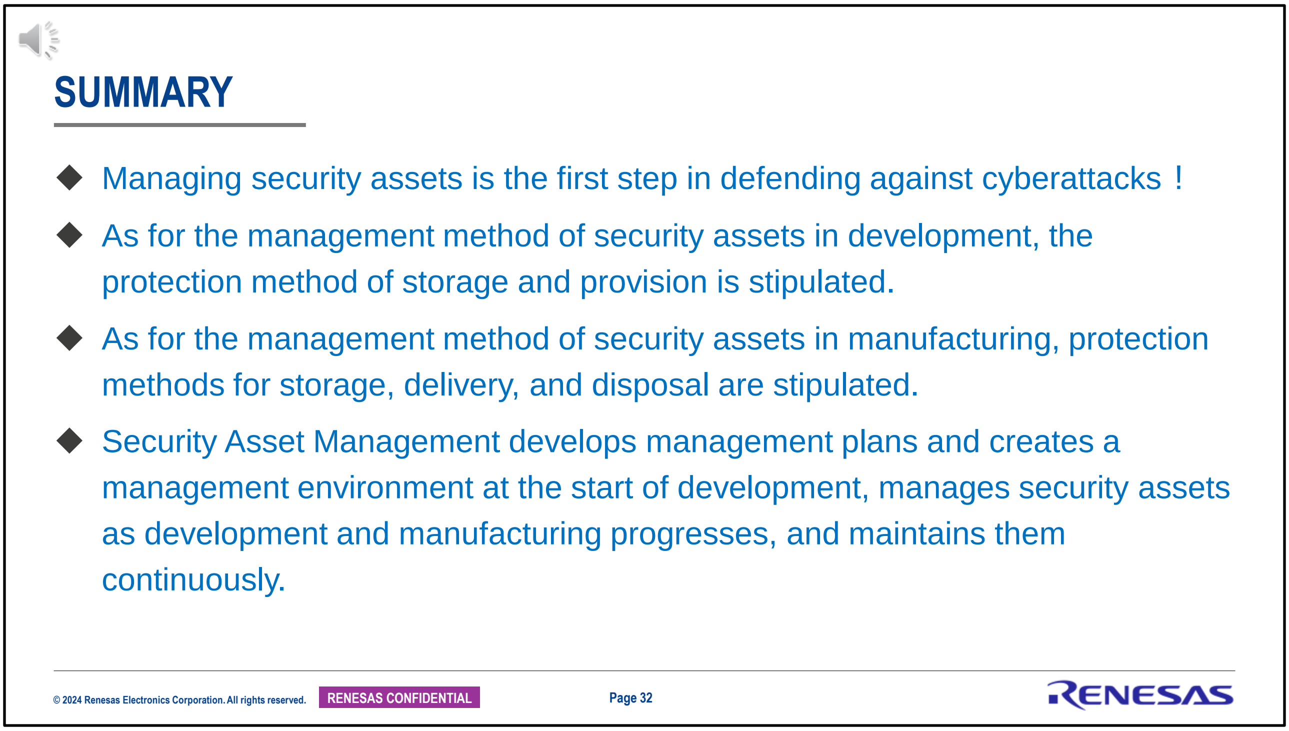
セキュリティに対応した製品開発を行うための標準類、当社のサイバーセキュリティポリシー、PSIRT、教育コンテンツに関する情報をまとめました。

https://renesasgroup.sharepoint.com/sites/REL-QSP-DQIPortal/SitePages/CyberSecurity.aspx

In addition, in this training, we only explained the outline of the security asset management operational regulations RCT-JB0026 and 0027, but the latest set of all other security-related technical standards and standards is posted on the cybersecurity site on the design quality portal. Please check this website for detailed rules.

4. SUMMARY

Chapter 4 is a overall summary.



SUMMARY

- Managing security assets is the first step in defending against cyberattacks！
- As for the management method of security assets in development, the protection method of storage and provision is stipulated.
- As for the management method of security assets in manufacturing, protection methods for storage, delivery, and disposal are stipulated.
- Security Asset Management develops management plans and creates a management environment at the start of development, manages security assets as development and manufacturing progresses, and maintains them continuously.

RENESAS CONFIDENTIAL

RENESAS

The four points written here are the summary of this educational module D, but if you have any questions after reading them, please go back to the relevant slides and review them one by one. Also, please be sure to read through the original standards RCT-JB0026 and 0027 that this education has summarized. As mentioned on page 2, those who need to qualify for a security role should take the included comprehension test and keep a snapshot of the page that shows a pass as proof of completion of the education.
Thank you for your attention.

Ver.	Date	Approval/making	Content
1.0	2021/2/5	Nagata/ Amimoto・Fujii QC Nakamura ・ Oba (P27~P30)	New making
2.0	2022/2/19	Nagata / Amimoto	Updated of contents according to RCT-JB0026 2nd edition. Updated of contents according to RCT-JB0027 2nd edition.
3.0	2024/6/3	Nagata / Amimoto	Updated of contents according to RCT-JB0026 4th edition.

Thank you